

*PB94-191202*

# **Federal Certification Authority Liability and Policy**

***Law and Policy of Certificate-Based Public Key and Digital Signatures***

**FILE COPY  
DO NOT TAKE**

**Michael S. Baum, J.D., M.B.A.**

Independent Monitoring  
Cambridge, Massachusetts USA

U.S. DEPARTMENT OF COMMERCE  
Technology Administration  
National Institute of Standards  
and Technology  
Gaithersburg, MD 20899







# **Federal Certification Authority Liability and Policy**

## ***Law and Policy of Certificate-Based Public Key and Digital Signatures***

**Michael S. Baum, J.D., M.B.A.**

Independent Monitoring  
Cambridge, Massachusetts USA

U.S. DEPARTMENT OF COMMERCE  
Technology Administration  
National Institute of Standards  
and Technology  
Gaithersburg, MD 20899

June 1994



**U.S. DEPARTMENT OF COMMERCE**  
**Ronald H. Brown, Secretary**

**TECHNOLOGY ADMINISTRATION**  
**Mary L. Good, Under Secretary for Technology**

**NATIONAL INSTITUTE OF STANDARDS  
AND TECHNOLOGY**  
**Arati Prabhakar, Director**



**ABSTRACT:**

This **FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY - *Law and Policy of Certificate-Based Public Key and Digital Signatures*** Report identifies diverse technical, legal and policy issues affecting a certificate-based public key cryptographic infrastructure utilizing digital signatures supported by "trusted entities." It examines potential legal implications, surveys existing legal paradigms and the structures and roles of relevant governmental agencies and presents various institutional approaches to controlling liability. It considers the underpinnings of a legal and policy framework which might serve as a foundation for security policies and their implementation and concludes with a series of recommendations, both general and specific.

**KEYWORDS:**

certificate-based public key cryptography, computer law, digital signature, electronic commerce, electronic data interchange, information security, liability, policy, trusted entities

**DATE:** June 1994





**METHODOLOGY:** This Report is the result of legal, business and security management research, interviews and analysis predominantly with public- and private-sector lawyers, policy makers, managers and management information system and security professionals in the United States and abroad.

**DISCLAIMER:** This report is not intended as legal advice nor as a substitute for legal counsel, although its contents provide a useful resource to the public key community. The National Institute of Standards and Technology (NIST) makes no claim or endorsement of the information provided.

**COPIES OF THIS REPORT:** Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA 22161, telephone +1 (703) 487-4650.

**ABOUT THE AUTHOR:** Michael S. Baum is *Principal* of Independent Monitoring, a consultancy focused on electronic commerce and information security law. He serves as a *Delegate* from the International Chamber of Commerce (ICC) to the United Nations Commission on International Trade Law (UNCITRAL); *Chair* of the EDI and Information Technology Division, Section of Science and Technology, American Bar Association (ABA) and its Information Security Committee; and *Chairman* of the ICC Working Party on Legal Aspects of Electronic Commerce.

The author solicits comments, criticism and dialogue from the readership.

Michael S. Baum  
Independent Monitoring  
33 Tremont Street  
Cambridge, Massachusetts 02139-1227 USA  
Tel: +1 (617) 661-1234  
Fax: +1 (617) 661-0716  
Net: baum@im.com





**"In particular, we must be able to deploy a  
public key infrastructure to support  
transactions across multiple networks."**

**Streamlining Procurement Through Electronic Commerce  
Federal Electronic Commerce Acquisition Team,  
President's Management Council Electronic Commerce Task Force  
Final Draft, April 29, 1994**



SUMMARY CONTENTS

- PREFACE.....iv

- ACKNOWLEDGMENTS.....viii

- TABLE OF CONTENTS.....ix

I. INTRODUCTION.....1

II. SCOPE.....2

III. DEFINITIONS.....4

IV. ASSUMPTIONS.....12

V. SURVEY OF FCA ACTIVITIES CREATING LIABILITY EXPOSURE .....22

VI. LEGAL CONSIDERATIONS .....79

VII. FCA INFRASTRUCTURE - PROPOSALS AND PARADIGMS.....161

VIII. SURVEY OF, AND APPROACHES TO, TRUSTED ENTITY LIABILITY .....235

IX. OTHER APPROACHES TO MITIGATE LIABILITY .....323

X. CONCLUSIONS AND RECOMMENDATIONS.....379

XI. APPENDICES.....388

XII. GLOSSARY.....410

XIII. INDEX.....414





## **PREFACE**

### **PURPOSE OF REPORT**

This Federal Certification Authority Liability and Policy Report (the "Report") identifies diverse technical, legal, and policy issues affecting a certificate-based public key cryptographic infrastructure. It is intended primarily as a reference source for information resource managers, policy and law makers in the public and private sectors, and lawyers and information security professionals who must understand and contribute to the planning, development, and use of a secure information infrastructure.

The Report assumes that it is in the interest of the federal government to identify, contemplate and develop programs and an infrastructure that not only satisfy its immediate internal needs but also fosters private sector development, cooperation and inter-operability. Therefore, the Report transcends purely public-sector issues and concerns to provide a viable resource for the public and private sectors, domestically and globally.

The Report first examines potential legal implications of certificate-based public key technology as they arise in terms of the various functions and roles that technology may be expected to perform. It then surveys existing legal paradigms, the structures and roles of relevant governmental agencies and other entities and various institutional approaches to controlling liability. As a whole, the Report presents the underpinnings of a legal and policy framework which can serve as the basis for security policies and their implementation. It contemplates aggressive and robust information security methods that exploit technologies, procedures and practices on the basis of their effectiveness and ultimate desirability. The Report concludes with a series of recommendations, both general and specific. Constructing information security requirements from a secure baseline is necessary to facilitate a cost-benefit analysis for relaxing certain requirements of that secure baseline.

Recognizing that there is a significant learning curve for all players and that major infrastructural change is indeed a multi-year undertaking, this Report considers both short-term and longer term (three to five years and beyond) issues and requirements. Fundamental architectural assumptions are constantly challenged and changing as we climb the learning curve of this relatively nascent technology. Consequently, it becomes increasingly difficult to predict the future. The explosion of Internet growth and demand for its commercialization, as well as the expanding scope of a proposed National Information Infrastructure (NII) have exceeded the pundits' most optimistic predictions. In response, this Report





provides a level of detail that is intended to provide for the uncertainties of future opportunities.

## **DIVERSE REQUIREMENTS DEMAND FLEXIBILITY**

A federal public key infrastructure must accommodate diverse requirements such that *security is commensurate with the contemplated risks*. Security requirements need not require the equivalent of Fort Knox to protect information of no greater value than a shoelace. Informal, personal transactions (which demand neither confidentiality nor nonrepudiation) generally require minimal security, whereas commercial transactions generally require more security, but frequently less than official government communications. Government communications are strictly official and require commensurate higher levels of security. Certain classes of information may require even stronger security.

Open systems threats have induced some proponents of Internet-based electronic commerce to demand "industrial strength" transactional security. Although the wisdom of providing such "industrial strength" security to *all* users, regardless of cost or their needs, is open to debate, the Internet is clearly unsuitable at present for official government messaging without enhanced security. Indeed, the government would need something of materially higher quality than the password access-based unencrypted security currently available on the Internet. A shift to open systems without appropriate security is unrealistic.

## **ROLE OF THE FEDERAL GOVERNMENT**

Interagency messaging within the federal government, being essentially a private management domain, can demand, provide and justify higher quality security. However, such security measures can and should demonstrate the viability of enhanced services for the private sector were government increasingly to promote a secure government-private communication standard consistent with government communications needs and policies. Indeed, a federal public key infrastructure might well serve to open new public and private opportunities and markets for computer-based commerce, ultimately expanding to serve millions of users. From technology life-cycle and development perspectives, public key may appear overly complex and not yet adequately commercialized to provide viable products, but this status should compel, rather than impede, the government to move aggressively toward solutions. There is presently a window of opportunity for government to influence public key infrastructure development that demands vision and demonstrable commitment.

In principle, government systems should not compete with private-sector initiatives. However, government does (or should) play an indispensable role in



influencing the direction of private infrastructure when it determines that the current direction is flawed, that there is a lack of direction, or that the private sector has failed (for example, because of excessive risk aversion or the "free-rider" problem) to undertake beneficial initiatives of national importance. In this regard, federal government messaging systems should be implemented to demonstrate future possibilities for the more risk-averse parts of the private sector.

A public key infrastructure can also contribute and catalyze the migration from traditional bilateral, pre-arranged trade agreements (such as electronic commerce "trading partner agreements") to more flexible, multilateral, potentially automated "systems-rules" arrangements that will better accommodate unfettered open communications and trade relationships. This migration in electronic commerce trade relationships requires a close partnership between the legal and security computer-based commerce communities of both the public and private sectors.

#### CONSIDERATION OF PRIVACY ENHANCED MAIL

This report uses Internet Privacy Enhanced Mail ("PEM") to exemplify certain properties and legal implications of certificate-based public key cryptography. PEM provides for a multi-level hierarchy of certification authorities, policy certification authorities and higher-level registration authorities that is both extensible (a potential benefit) and complex (a potential detriment). These qualities make PEM a useful model for comparative analysis.

Similarly to PEM, for example, a central element of most federal public key infrastructure proposals is an administrative function or entity called a *certification authority*. A certification authority is a "trusted entity" responsible for creating the "binding" between an entity and its public key in the form of a public key certificate.

PEM is also considered and emphasized because of its comparatively advanced stage of development and the availability of extensive documentation and commentary (via e-mail and RFCs) concerning its architecture, implementations, inter-operability, policies and risks. Moreover, PEM was initially federally funded and continues to evolve with significant social and economic benefit. Nevertheless, the Report's focus on PEM is not necessarily an endorsement of PEM to the exclusion of other approaches, architectures and implications.





## **ARCHITECTURAL-LEGAL INTERFACE**

The relationship and more practical considerations among architecture and the law is both intriguing and complex. Certain public key advocates have proposed a rather flat and more centralized architecture, urging that shorter paths are "easier," more viable and practical for accommodating the diverse requirements of the personal, commercial and governmental transactions noted above. Other advocates have urged that all major employers and certifying bodies will inevitably become CAs. The trade-off is between longer paths (implicating a multi-level hierarchy) and more CAs (implicating a "shallow" hierarchy; and "peers"). Therefore, complexity will invariably be introduced. With architectural complexity, however, comes legal complexity (and uncertainty). One of the foremost challenges of the Report has been to set forth actual and potential legal norms that are capable of application to varying levels of architectural complexity.

## **STANDARDS AND CRYPTOGRAPHIC POLICY**

This Report reflects sensitivity to the government's relative acceptance, adoption, promotion, or rejection of certain standards and its evolving relationship with regional and international security and information technology policy developments. The state and direction of federal involvement in such relationships will certainly influence the future. Finally, the developing infrastructure should not, and cannot, be considered in isolation from the current debates concerning cryptographic export policy, intellectual property rights and escrow-based encryption technologies (escrow technology may affect system designs as profound as has public-key technology -- and its full ramifications are unknown). Indeed, these issues have had a destabilizing impact on certain public key developments (as well as, in some cases, stimulating creative thought and proposals to move forward).

The many issues raised in the Report demonstrate both a lack of, and need for, intensive coordination, research, development and implementation. The Report is intended to provide a framework to promote the coordination necessary to solve these complex and elusive problems.

M.S.B.



## ACKNOWLEDGMENTS

Special thanks are given for the editorial assistance of Locke R. McMurray (Harvard Law School, LL.M.). The suggestions, insights and editorial comments on portions of the Report by the following people are gratefully acknowledged: Thomas Armstrong, Esq. (GAO); Ted Barassi, Esq. (Nat'l Law Center For Inter-American Free Trade); Elaine Barker (NIST), Shimshon Berkovits, Ph.D. (MITRE); D. James Bidzos (RSADSI); Dennis Branstad, Ph.D. (NIST); Harold Burman, Esq. (U.S. Dep't of State); Prof. James E. Byrne (George Mason Law School); Chuck Chamberlain (USPS); George Chandler, Esq. (Hill, Rivkin, Lomberg, O'Brien, Mulroy & Hayden); Jerry Cohen, Esq. (Perkin, Smith & Cohen); Thomas R. Cornwell (Chubb); Hon. Bertram R. Cottine (Nat'l Consumer Product Safety Comm'n) Sandy Epstein (Racal-Guardata, Inc.); Prof. Carl Felsenfeld (Fordham Law School); Marty Ferris (U.S. Treasury); Richard Field, Esq.; Stephen Fishbein, Esq. (Shearman & Sterling); Robin Jo Frank, Esq. (U.S. Department of State); Judy Furlong (MITRE); Don Ghostlaw, Esq. (Aetna); M. Blake Greenlee (M. Blake Greenlee Associates); Eugene E. Hines, Esq. (American Society of Notaries); Dr. Roland P. O. Hüber (CEC); David Hough (N. Am. Trade Pt.); Bruce Hunter, Esq. (G.E. Information Services); Barbara Jacobs, Esq. (SEC); Steven Kent, Ph.D. (BBN); Richard C. Koenig ((ISC)<sup>2</sup>); Jim Kolouch (FBI); Prof. Boris Kozolchyk (U. of Arizona College of Law); Peter Landrock, Ph.D. (Cryptomathic); Susan A. Laniewski, Esq. (National Center for State Courts); Marc Lauritsen, Esq. (Harvard Law School); John Lowry (BBN); Alfred I. Maleson (Professor of Law, *Emeritus*, Suffolk Law School); Herbert Marks, Esq. (Squires, Sanders & Dempsey); Sead Muftic (COST); F. Lynn McNulty (NIST); Notaio Dott. Mario Miccoli (Unione Internazionale Del Notariato Latino); Charles J. Miller, Esq.; Andrew Mozina, Ph.D.; Norman R. Nelson, Esq. (NYCHA); Larry D. Nelson (AT&T); William Nelson (NACHA); Dwight C. Olsen (Data Securities Int'l); George Parsons (RSADSI); Eric W. Pearson (Student, Harvard Law School); Michel Peereman (Belgian Nat'l Fed. of Chambers of Commerce); Blanche Petre, Esq. (S.W.I.F.T.); Leon A. Pintsov, Ph.D. (Pitney Bowes); Cheryl Posegay (Student, Boston Univ. Law School); Jerry Rainville, Esq. (NSA); Laurence H. Reece, III, Esq. (Heidlage & Reece, P.C.); Peter Robinson (USCIB); Robert Rosenthal (NIST); Jeff Schiller (MIT); Laurence Shomo (NASA); Miles E. Smid (NIST); Hon. Renaud Sorieul (UNCITRAL); Jeff Stapleton (MasterCard); Frank W. Sudia, Esq. (Bankers Trust); George Usher (Financial Management Services); Joe Wackerman, Esq. (USPS); Peter Waegemann, Ph.D. (Medical Records Inst.); Peter Weiss, Esq. (OMB); Al Williams (GSA); and Peter Williams (NASA/Sterling Software).





# TABLE OF CONTENTS

PREFACE .....	iv
ACKNOWLEDGMENTS .....	viii
I. INTRODUCTION .....	1
II. SCOPE .....	2
III. DEFINITIONS .....	4
IV. ASSUMPTIONS .....	12
A. Organizational Status of the FCA.....	12
B. Relationship Among CA Users .....	12
C. Information Requirements .....	12
D. Availability.....	16
E. Support for Non-Repudiable, One-Time, Discrete Transactions.....	16
F. Diverse Applications.....	16
G. Privilege.....	17
H. Consumer Transactions.....	18
I. Open Systems .....	19
J. Government Consent to Be Liable .....	20
K. International Root Authorities .....	20
L. Use of Card Technologies.....	20
V. SURVEY OF FCA ACTIVITIES CREATING LIABILITY EXPOSURE .....	22
A. FCA Organization and Roles.....	23
A.1. Primary Roles of the FCA .....	23
a. Policy and Procedures Creation.....	23
b. Certificate Creation.....	23
c. Accreditation .....	23
d. Auditing.....	24
e. Software, Hardware, or Service Developer .....	25
A.2. Secondary Roles of the FCA .....	25
a. Communications (Voice and Data).....	25
b. Time and Date Stamping .....	25
c. Directory Services .....	26
d. Education and Training.....	26
e. Insurance.....	27
f. Billing for Certificates, CRLs.....	27
g. Dispute Resolution Mechanisms.....	27
h. Key Generation.....	27
i. Management of Keys.....	28
A.3. Administration and Management .....	29
a. Criteria for, and Oversight of, Upper-Level Management .....	29
b. Criteria for, and Oversight of, FCA Employees .....	30
c. Establishing Personal vs. Entity Liability .....	31
d. Inadequacies of Sanctions Against FCA Employees .....	31
e. Delegation.....	32
f. Communities of Interest.....	32
A.4. Relationships Among the FCA and Other Parties.....	33
a. Governmental Providers of FCA-Related Services.....	34
b. Third Party Service Providers .....	34
c. Government Users .....	34
d. Private Users.....	34
e. Non-FCA Certification Authorities and Hierarchies .....	34
f. International Relationships.....	34



A.5. Communications.....	35
a. Certificates .....	35
b. Notices .....	35
c. Directory Information.....	36
d. Identity and Locality Information on Other FCA Entities.....	36
e. Policies Statements and Agreements.....	36
f. Attribute Certificate-related Information.....	36
A.6. Establishing FCA Expectations .....	36
a. FCA Policy Development .....	37
b. Issuing Certificates.....	38
c. Hierarchical vs. Distributed Trust Models.....	39
d. Availability .....	39
A.7. Intellectual Property Protections.....	41
a. User Identification (Including Name) Information.....	42
b. Algorithms .....	42
c. Technical Specifications.....	42
d. Certificates and CRLs .....	43
e. Public and Private Keys.....	43
f. Digital Signatures.....	43
g. Standards.....	43
h. Hardware and Software .....	43
i. Directory Services .....	43
A.8. Duty to Assist or Enforce.....	43
a. Investigations and Production of Evidence.....	44
b. Criminal.....	44
c. Establishing Non-FCA Secure Environments .....	44
A.9. Capitalization.....	45
a. Sufficient Capitalization.....	45
b. Legislative or Administrative Limitations .....	45
c. Commercial Insurance .....	45
d. User, Member, or Agency Indemnification.....	45
e. Risk Pools .....	45
B. The Certificate Application Process.....	46
B.1. Completeness & Propriety of Certification Request Data.....	46
a. Applicant Identification Information .....	46
b. Direct/Internal Applicant Certification (Verified by FCA).....	49
c. Remote Applicant Certification (Verified by Notary).....	49
d. Humans vs. Organizations vs. Devices .....	49
B.2. Proof and Verification of CRD.....	50
a. Trustworthiness of Verifier .....	50
b. Investigation.....	51
c. Authentication vs. Authorization .....	51
B.3. Naming.....	52
a. Subject-Name Uniqueness .....	52
b. Name Subordination.....	54
c. Accommodating User-Requested Naming.....	55
d. Authority to Use Organizational Affiliation.....	55
e. Right or Privilege .....	55
f. Communities of Interest.....	55
g. Naming Registration Authorities .....	55
h. Numbering.....	57
B.4. Certificate Application Processing .....	57
a. Timeliness and Accuracy.....	57





b. Nondiscrimination and Fairness.....	58
c. Retention of CRD and Other Information.....	58
d. Billing and Accounting .....	59
e. Audit Journal.....	60
f. Dispute Resolution Procedures .....	60
C. Certificate Generation.....	60
C.1. Strength of Certificate.....	60
a. Algorithm .....	60
b. Meaning/Significance of Certificates.....	61
c. Interworking.....	61
d. Other/Environmental Factors.....	61
C.2. Certificate Validity Period .....	61
a. Use Prior, During and Following Validity Period.....	61
b. Duration .....	61
C.3. Certificate Issuance Propagation .....	62
a. Push vs. Pull .....	62
b. Extensions and Reissuance.....	62
c. Automation (Minimizing Human Involvement).....	63
C.4. Attribute and Other Certificates.....	64
a. Delegation Certificates.....	65
b. Virtual Certificates .....	65
c. Sponsor Certificates.....	65
d. Other Certificates .....	65
e. Different Keys/CAs for Authentication & Attribute Certificates.....	66
f. Certified Time Stamps.....	66
g. Liability for Information Content.....	67
C.5. Controls for Certificate Generation.....	67
a. Prevention of Forgery .....	67
b. Audit Trail .....	68
c. Retention of Current or Expired Certificates.....	68
d. Confidentiality of Certificates.....	68
D. Certificate Revocation .....	68
D.1. Authority to Request and Revoke Certificates .....	68
a. Delay/Failure to Submit a CRL Request.....	69
b. Revocation of Employee Certificate upon Employer Request.....	69
c. Revocation of Certificate upon Request of Subject's Agent .....	69
d. Law Enforcement.....	69
D.2. Basis for Issuing CRL.....	69
a. By the FCA.....	70
b. By the User .....	71
D.3. Proof and Verification of CRL Requests.....	72
a. Investigation of Validity and Authenticity.....	72
b. Establishment and Adherence to CRL Request Rules .....	72
D.4. CRL Keys .....	72
a. Use of Different Keys for CRL and Certificate Issuance.....	72
D.5. CRL Validity Period .....	72
a. Nature of Activity .....	72
b. Specificity.....	72
c. Non-Repudiation vs. Origin Authentication.....	73
D.6. CRL Updating and Promulgation.....	74
a. Push .....	74
b. Pull.....	74
c. Scheduled .....	75



d. Unscheduled .....	75
e. Garbled, Lost, Delayed and Misrouted CRLs & CRL Requests .....	76
f. Reason Codes for CRL Issuance .....	76
g. Availability of Global CRL Data Base to Users .....	76
D.7. CRL Retention .....	77
a. Archival Methods .....	77
b. Time and Date Stamping .....	78
c. Revision of Retention Policies .....	78
VI. LEGAL CONSIDERATIONS .....	79
A. Purpose and Policies of Liability .....	79
B. Legal Infrastructure of the FCA .....	83
C. Certification Liability .....	91
1. Contract or Tort? .....	92
2. First-Level Certification Liabilities .....	92
a. Non-Certification .....	92
b. Misrepresentation by the User .....	94
Table 1 - Liability for Unauthorized Use of Authen. Instrument .....	95
c. Misrepresentation by the CA .....	98
3. Second-Level Certification Liabilities .....	106
a. Direct Liability in Tort or Contract .....	106
b. Vicarious Liability .....	107
D. General Contract Liability Considerations (Including Damages) .....	109
1. Applicability of the U.C.C. .....	109
2. Warranties Under the U.C.C. ....	111
3. Remedies .....	117
a. Direct Damages .....	118
b. Consequential Damages .....	119
c. Specific Performance .....	123
d. Rescission .....	123
4. Limitations on Remedies .....	124
a. Limitation on Consequential Damages .....	124
b. Liquidated Damages .....	125
c. Punitive Damages .....	126
E. General Tort Liability Considerations .....	126
1. Liability for Defective Information Technology .....	127
2. Liability for Defective Information Technology (Strict Liability) .....	129
3. European Directives .....	133
4. Negligently Undertaking to Provide Security .....	134
5. Professional Negligence .....	134
6. Gross Negligence .....	136
7. Punitive Damages .....	136
F. Subsidiary (Civil) Liability Issues .....	136
1. Anti-Competitive Considerations .....	136
2. Defamation .....	139
3. Interference with Contractual Relations .....	141
4. Invasion of Privacy .....	142
G. Criminal Liability .....	144
1. Computer-Related Crime Generally .....	145
2. Survey of Computer Crime Statutes .....	147
3. Survey of Relevant Non-Computer-Specific Statutes .....	153
4. Summary .....	160
VII. FCA INFRASTRUCTURE - PROPOSALS AND PARADIGMS .....	161
A. The Federal Government as Provider of FCA Services .....	161





1. Constitutional Issues.....	161
a. Separation of Powers.....	163
b. FCA Threats to the Constitutional Rights of Persons.....	168
2. Authorization to Expend Funds .....	170
3. Liability of the Federal Government Generally.....	174
a. Federal Tort Claims Act.....	175
b. The Tucker Act .....	182
c. The Administrative Procedure Act .....	185
d. Privacy Act.....	187
4. Notable FCA Candidates .....	191
a. United States Postal Service .....	191
b. Federal Reserve System.....	203
c. General Services Administration.....	210
d. National Institute of Standards and Technology .....	212
e. Other Domestic Entities .....	213
5. International Organizations Generally .....	214
a. Privileges and Immunities .....	216
B. The Federal Government as Contractor for FCA Services .....	223
1. Federal Contractor Liability .....	223
2. Federal Contracting/Federal Acquisition Regulation.....	225
VIII. SURVEY OF, AND APPROACHES TO, TRUSTED ENTITY LIABILITY .....	235
A. Banks and Financial Services.....	235
1. U.C.C. Articles 3 and 4 (Checks) .....	235
a. Matters Related to Signature Verification.....	235
b. Failure to Observe Customer Instructions .....	237
c. Duty of Care and Measure of Damages.....	238
d. Specifically Electronic or Computer-Related Matters.....	240
2. U.C.C. Article 4A.....	240
a. The Role of Security Procedures .....	241
b. Errors and Delays.....	243
3. Automated Clearing Houses.....	249
4. The New York Clearing House Association and CHIPS .....	254
5. Fedwire .....	258
6. S.W.I.F.T.....	260
7. Special Risk Allocation Schemes - Consumer Transactions .....	262
a. The Electronic Fund Transfer Act.....	263
b. Truth-in-Lending Act and Credit Cards.....	267
Table 2 - Credit Card .....	269
B. Value Added Networks .....	269
Table 3 - Comparison of VAN Liability Caps.....	273
C. Escrow and Other Legal Agents .....	276
1. Escrow Agents.....	276
2. Trustee and Trustor .....	278
3. Bailor - Bailee Relationship.....	280
4. Insurance Agent-Insured .....	281
5. Vault & Safe Deposit Boxes.....	281
D. Notaries Public .....	282
1. Introduction.....	282
2. Applications and Relevance .....	282
a. "Remote" FCA Notaries.....	283
Figure 1 - Notary Facilitation of Remote Certificate Application	
Process.....	284
b. Notaries Internal to the CA.....	284



Figure 2 - Notary Internal to Certification Authority.....	285
3. Notarial Independence.....	285
4. Model for FCA Conduct and Procedures? .....	287
5. Liability.....	287
6. Notarial Law Reform.....	288
7. The Case for the "Super Notary" .....	289
E. Chambers of Commerce.....	291
1. CEDI-FACT / FAST.....	291
2. ATA Carnet.....	293
3. Certificate of Origin.....	294
F. Department of State (Passports).....	294
G. Common Carriers .....	297
1. Regulation of United States Telecommunications.....	299
2. Regulatory Regimes Abroad.....	305
a. Recognized Private Operating Agencies.....	305
3. Operators of Transport Intermediaries in International Trade.....	307
4. The Hague, Hamburg, and Other Rules .....	311
5. Bills of Lading .....	315
6. Liability of "Warehousemen" for Title Information.....	317
H. Securities Rules.....	319
1. EDGAR.....	319
2. Electronic Display Books.....	320
3. BEACON.....	320
I. CommerceNet.....	322
IX. OTHER APPROACHES TO MITIGATE LIABILITY .....	323
A. Certification and Accreditation.....	323
Figure 3 - Integration of Certification and Accreditation.....	326
1. Entities.....	326
2. Professionals.....	327
3. Products and Services.....	329
4. National Voluntary Laboratory Accreditation Program.....	330
5. Quality Certification and ISO 9000.....	331
6. Certification and Accreditation Liabilities.....	333
7. Potential FCA Accreditation and Certification Bodies .....	333
Table 4 - Accreditation and Certification Matrix .....	336
8. Other.....	337
B. Insurance .....	337
1. Defined.....	337
2. Assessing Insurance Risks .....	338
3. Government Insurance Programs.....	340
4. Private Insurance.....	343
5. Fidelity Bonds .....	344
6. Self Insurance.....	345
7. Conclusion.....	347
C. Policy Statements and Agreements.....	347
1. Demand for Agreements and Policy Statements.....	347
Figure 4 - Hypothetical FCA Legal Structures/Relationships .....	349
Table 5 - Entities Identified .....	350
Table 6 - Possible Agreements and Policy Statements Identified .....	351
Table 7 - Possible Coverage of Policies and Agreements .....	352
2. Policy Statements.....	352
Table 8 - Policy Statements Compared.....	356
3. Model Policy Statement Development.....	357





4. Model Agreements.....	358
5. Conclusion.....	359
D. Miscellaneous Initiatives.....	361
1. Draft ABA Model Global Public Key Infrastructure Rules of Practice.....	361
2. UNCITRAL EDI Statutory Provisions .....	361
a. Security Requirements.....	363
Table 9 - Security Requirements Compared.....	364
Table 10 - Costs and Benefits of Security Standards.....	368
Table 11 - Survey of Security Definitions .....	371
b. Variation by Agreement .....	371
c. System Rules Issues.....	375
3. Security-Relevant Standards.....	377
4. Alternative Dispute Resolution Mechanisms .....	378
X. CONCLUSIONS AND RECOMMENDATIONS.....	379
A. Forge Ahead with an FCA Implementation.....	380
B. Include Legal Goals in Criteria for FCA Pilots .....	380
C. Promote the Study and Development of Legislative Proposals.....	380
D. Develop FCA Agreements and Policies.....	381
E. Aggressively Promote a Rationalization of the Global Certificate Infrastructure.....	382
F. Organizational Structure.....	382
G. Develop an Appropriate Interface Between the FCA, Other Federal Organizations and Private Third Party Service Providers, Including Non-FCA Certification Hierarchies.....	383
H. Develop Special Presumptions for FCA-Enhanced Communications.....	383
I. Develop an FCA Infrastructure that Limits, Rather than Excludes, Liability .....	383
J. Develop an FCA Infrastructure that Provides Flexible Liability Limits.....	384
K. Utilize Card Technologies in Early Pilots .....	384
L. Identify and Implement Requisite and Appropriate Disclosure, Notification and Warning Mechanisms.....	384
M. Evaluate Insurance Paradigms.....	385
N. Evaluate and Reform Computer Crime Laws.....	385
O. Assure the Accountability of Employees in Positions of Trust .....	385
P. Integrate Legal Risk Analysis into FCA Risk Analysis.....	386
Q. Promote and Integrate Audit, Legal and Security Education Extensively.....	386
R. Research the Implications for Consumer Use of the FCA.....	386
S. Develop (or Bolster) a Multidisciplinary FCA Development Group .....	387
T. Promote and participate in Attribute Certificate Methodologies.....	387
U. Recommendations for Further Work .....	387
XI. APPENDICES.....	388
Appendix A - Linking Security .....	388
Appendix B - "The EDI Clearinghouse" .....	389
Appendix C - "The Automation of the Notary Public" .....	390
Appendix D - RSA/Apple A.O.C.E. Certificate Application Form .....	391
Appendix E - Sample Policies.....	392
Appendix E.1. - M.I.T "Mid-Range" Policy Statement .....	392
Appendix E.2. - RSADSI "Low Assurance" CA Policy Statement.....	394
Appendix E.3. - T.I.S. Commercial PCA Policy Statement.....	399
Appendix E.4. - COST Int'l Consortium PCA Policy Statement .....	402
Appendix E.5. - RFC 1422 Outline for PCA Policy Statements .....	406
Appendix F - Lloyds Computer Insurance Policy .....	408
XII. GLOSSARY .....	410
XIII. INDEX.....	414



# FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY

## *Law and Policy of Certificate-Based Public Key and Digital Signatures*

**Michael S. Baum, J.D., M.B.A.**

### **I. INTRODUCTION**

This Report surveys potential liabilities as well as liability and policy issues, that might arise in the operation of a Federal Certification Authority ("FCA")<sup>1</sup> infrastructure. The FCA, if established, is contemplated to perform various certificate-based public key cryptographic services to provide trustworthiness and reliability to the communications of diverse FCA users. This Report also considers the procedures, processes and technologies associated with certificate issuance, maintenance and revocation, and explores the extent to which those functions may affect user expectations and FCA liability. In general, the FCA's structure and the scope of its activities raise issues and potential legal consequences based in contract, tort, constitutional, and criminal law that will need to be resolved as the FCA develops. Recognizing that liability will be a function of the actual service offerings, as well as other currently undecided issues, this Report is necessarily somewhat speculative and will consider potential liabilities for a broad range of possible implementations.

To the extent that implementation of the FCA is a pioneering effort undertaken without the benefit of a comprehensive legal framework, considerable effort is made here to identify and evaluate existing entities which enjoy a rich legal infrastructure and which provide useful legal paradigms. This effort identifies particularly those entities which have seriously grappled with information in electronic form. Extrapolation from such existing institutions and their legal infrastructures is unavoidable and often quite useful, but it must also be acknowledged that this usefulness may be limited in certain cases.

Most importantly, this document is intended as an "issues-and-think piece" to foster debate over the nature and extent (actual and optimal) of FCA liability. Many key issues surrounding FCA liability have yet to be resolved or even comprehensively articulated. But while definitive analysis and solutions remain out of reach for the time being, it is hoped that this Report will advance the discussion and facilitate additional intensive analysis and research. Significant work lies ahead.

---

<sup>1</sup> "FCA" is considered above in the Preface and defined below in Section III., "Definitions."



## II. SCOPE

An attempt to survey the liabilities associated with an infrastructure that is still largely undefined would effectively require the review of a nearly infinite number of issues. This Report attempts to narrow the range of issues by curtailing the analysis of end-user-to-end-user liabilities and focusing instead on the potential liabilities of the FCA vis à vis the various users of FCA services.<sup>2</sup>

Because the FCA's organizational structure is as yet indeterminate, this Report also considers liability issues from both private and public perspectives. Making analogies with legal structures in the private sector is a necessity by default and enriches the analysis, particularly since there is little or no directly relevant legal precedent addressing FCA activities.

The planning and development of an FCA infrastructure will benefit from consideration of diverse technical, procedural and administrative approaches and solutions. Accordingly, diverse and extensive background materials are provided to give perspective to, and lay a foundation for, future work. This Report touches upon a multitude of materials to provide useful resources and education to the diverse players (both legal and nonlegal) who must grapple with these issues and who will contribute to the development of the FCA infrastructure.

This Report begins with some critical definitions that pertain to relevant legal standards. Second, it presents a series of guiding assumptions that incorporate the few fixed points of reference of legal import in this exceedingly unfixed field. Third, it surveys the universe of potential FCA activities that create liability exposure, particularly with respect of the FCA's provision of authentication and integrity assurance services. Although constitutional privacy issues associated with certificate-based public key cryptography are real and substantial, this Report concentrates only on those privacy issues surrounding the certificate application

---

<sup>2</sup> Useful materials to consider in evaluating end-user-to-end-user liability issues in electronic commerce are treated in various model EDI agreements, *see, e.g.*, EDI AND INFO. TECHNOLOGY DIV., SECTION OF SCIENCE AND TECHNOLOGY, AM. BAR ASS'N, MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY (1992), white papers, *e.g.*, Michael Baum, Linking Security and the Law of Computer-Based Commerce (Workshop on Security Procedures for the Interchange of Electronic Documents, NISTIR No. 5247, Nov. 12-13, 1992) [hereinafter LINKING SECURITY] (reproduced as Appendix A, *infra*), texts, *see, e.g.*, M. BAUM & H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW (Wiley, 1991) [hereinafter ELECTRONIC CONTRACTING], and reports, *e.g.*, Good Security Practices for Electronic Commerce, Including Electronic Data Interchange (NIST Special Pub. No. 800-9, Dec. 1993).



process and related support services.<sup>3</sup> Fourth, relevant theories of liability are identified and their potential as a basis for FCA liability considered. Fifth, the role of the federal government as such in the FCA is considered, both in terms of exploring the existing authority of potential candidates to undertake such activities and of the unique liability considerations implicated thereby. Sixth, liability apportionment schemes for various public and private institutions which provide *trusted entity functionality* are examined and, where appropriate, evaluated for their potential relevance and desirability for the FCA. Seventh, the role of certification activities generally and various mechanisms to limit or manage liability are examined. The Report concludes with a series of preliminary recommendations. A number of supplemental documents and sample materials are attached as Appendices.

---

<sup>3</sup> See, e.g., *infra* Sections VI.F.4. ("Invasion of Privacy") and VII.A.3.d. (concerning the Privacy Act).

### III. DEFINITIONS

To limit confusion, and to augment the predictability of potential liabilities, the FCA infrastructure should adopt concise and appropriate definitions.<sup>4</sup> This

---

<sup>4</sup> The author recognizes that the confusion which invariably plagues domestic and international security-related standards bodies stems in substantial part from a lack of consistent definitions. Consequently, certain terms defined herein contain subtle variances from terms used in different domestic and international standards. Eliminating these inconsistencies is particularly important when defining legal rights and responsibilities, especially in the context of information security.

There has been a trend in the development of definitions for certificate-based public key standards and guidelines, as well as in the law,

... to reach for that most fundamental of references -- the dictionary -- and seek an apparently neutral definition of a critical word or phrase. Increasingly, the [Supreme Court] justices are doing just that.

An informal survey reveals that, in decisions announced between Jan. 1992, and May 17, 1993, the justices recited dictionary definitions of key phrases 54 times in 38 cases, drawing on 23 different dictionaries. About half the definitions came from legal dictionaries, with the rest pulled from a variety of general compendia.

By contrast, in 1951-52 the Court recited dictionary definitions in opinions in only four cases.

This emerging jurisprudence of lexicography prompts a number of questions...

Is the Supreme Court dictionary-shopping through scores of lexicographic volumes, searching for that perfect definition? Do certain justices rely on cherished dictionaries that were perhaps won in debate contests of their youth? ...

Back in 1951, Justice Frankfurter [stated in *Dennis v. U.S.*, 341 U.S. 494 (1951):] 'The First Amendment is to be not read as barren words found in a dictionary but as symbols of historical experience.'

D. Stewart, *By the Book: Looking up the law in the dictionary*, A.B.A. J., July 1993, at 46-47.

Incidentally, the so-called "Dictionary Act" contains a number of definitions that warrant review prior to general implementation of public key cryptography. For example, "signature" is defined to "include[] a mark when the person making the same intended it as such" and "writing" is defined to "include[] printing and typewriting and reproductions of visual symbols by photographing, multigraphing, mimeographing, manifolded or otherwise." 1 U.S.C. § 1. The "tactile" orientation of these definitions, which have not been amended since their adoption in 1948, is obvious.

section defines or comments upon certain important terms which have been the subject of confusion in the information security, electronic commerce and legal communities. In some cases, these definitions reveal problems implicit in defining FCA-related matters. The proposed definitions or comments chosen for the terms below are intended to reduce confusion and to provide a model for the consideration and resolution of other important definitions.

**-Assurances:** Statements or conduct intended to convey the general intention, supported by good faith efforts, to provide the services specified, rather than an unequivocal commitment to perform fully and satisfactorily.

"Assurances" are to be distinguished from the provision of insurance, guaranties, or warranties unless otherwise expressly indicated.

**-Certification Authority:** An entity "trusted by one or more users to create and assign certificates."<sup>5</sup> Whether, and to what extent, the FCA "certifies" something or simply *registers* something requires articulation.<sup>6</sup>

"Certification" is to be distinguished from the provision of insurance, guaranties, or warranties unless otherwise expressly indicated.<sup>7</sup>

---

For relevant security standards which contain useful definitions lists, see Section IX.D.3. below. *See* Section IX.D.3., *infra* (referencing relevant security standards that contain useful lists of definitions).

<sup>5</sup> ITU-T, X.509 § 3.3. (1993). The X.509 definition permits certification authorities to "create the user's keys"; *cf.* Section V.A.2.h., *infra* (concerning key generation). A "certificate" is a digitally signed data structure that binds an entity's name (or identity) with its public key. It has also been defined as "[t]he public key and identity of an entity together with some other information, rendered unforgeable by signing it with the private key of the certifying authority which issued it." American National Standards Institute (ANSI) X9.30-199X PUBLIC KEY CRYPTOGRAPHY - USING IRREVERSIBLE ALGORITHMS FOR THE FINANCIAL SERVICES INDUSTRY, PART 3: CERTIFICATE MANAGEMENT FOR DSA, § 2.1., at 2 (draft March 15, 1994) [hereinafter ANSI X9.30].

<sup>6</sup> In general, this paper assumes that the FCA will engage in "certification" to ensure completeness of its coverage of liability issues. "Registration" activities would expose the FCA to considerably less risk.

<sup>7</sup> In the context of Internet's Privacy Enhanced Mail (PEM) implementation, concern has been expressed that "the term 'certification' . . . could be construed to imply some kind of guarantee with respect to the agent whose certificate is signed by the Internet Society. There are potential liabilities associated with any such implied certifications and it is thought that an alternative term such as . . . Certificate Registration Authority or something using the neutral term



**-Digital Signature:** "[A] non-forgable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data."<sup>8</sup> A digital signature does not necessarily imply the satisfaction of all legal requirements that are normally satisfied by conventional holographic signatures. The FCA and/or its users should define the precise uses and implications of a digital signature.<sup>9</sup>

**-Escrow; Escrow Agent:** If the FCA provides key generation services, or if FCA functions must accommodate "Clipper"-related infrastructures, the use and meaning of the terms *escrow* and *escrow agents* requires determination. Choosing the precise name for the entities that would be entrusted with

---

'registration' would be a material improvement." V. Cerf, Email posting (May 5, 1992); *see infra* Section V.1.D., *infra* (discussing express warranties).

<sup>8</sup> NIST, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FIPS PUB 140-1 (May 24, 1993). A digital signature has also been defined as "[d]ata appended to, or a cryptographic transformation of, a data unit [e.g., a document] that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient." SECURITY ARCHITECTURE, ISO 7498-2-1988(E). One further (evolving) definition under development within the Information Security Committee, *see infra* note 129, that seeks to accommodate both legal and security communities is:

a number that is created as a function of the (i) information content of a record (in digital format) to be signed and, (ii) identity of its signer as represented by the signer's unique private key (number).

In a public key cryptosystem, it is anticipated that each user will generate (or will be assigned) a key "pair" that has two inverse components -- a private key and a public key. The system is designed such that one component can be made public (the public key, along with other identifying information) without compromising the other component (the private key). The private component, known only to the user (unless generated by the CA), is used to *sign* outgoing messages. The public key is distributed to other users with whom the sender plans to exchange messages or files, and is used to verify authenticity of the sender's message. Thus, users can communicate securely without having previously exchanged keys.

<sup>9</sup> *See* LINKING SECURITY, *supra* note 2, § II.c., at 39 *et seq.* The precise use of a digital signature can be expressed in various ways, including "meaning encoding" within messages (*see* ANSI X12.58 version 2), certificates, policy statements and agreements.



holding cryptographic keys has generated confusion and contention.<sup>10</sup> This Report will continue to use the expressions *escrow* and *escrow agent* to signify the role of one who holds information subject to certain duties.

---

<sup>10</sup> The Clinton Administration's Clipper-chip proposal defined the intended key-component holders as *escrow agents*. "Key escrow" was defined in the proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES), 58 Fed. Reg. 40,791 (July 30, 1993) as: "A process involving transferring one or more components of a cryptographic key to *one or more* trusted key component escrow agents for storage and later use by government agencies to decrypt ciphertext if access to the plaintext is lawfully authorized." (emphasis added). The ESS was approved as FIPS PUB 185, 59 Fed. Reg. 5,997 (Feb. 9, 1994) where the definition of "key escrow" was updated to: "The process of managing (e.g., generating storing, transferring, auditing) the two components of a cryptographic key by two key component holders." FIPS PUB 185 at 3. See Lewis, *Of Privacy and Security: The Clipper Chip Debate*, N.Y. TIMES, Apr. 24, 1994, at F5; ASC X9F, *Guideline X9.TG-11-199X, Using Capstone in Financial Systems: An Application Programming Interface*, N9-94 (Apr. 4, 1994).

Some groups argued that an escrow agent must be independent from the parties and that therefore the government could not serve as its own escrow agent. The definitional dispute, however, appears to be a semantic one only. See NIST, Cryptographic Issue Statements Submitted to the Computer System Security and Privacy Advisory Board (May 27, 1993) (addressing the "Clipper-Chip" proposal); Section VIII.C. ("Escrow and Other Legal Agents"), *infra*. Cf. Section VII.A.1. ("Constitutional Issues"), *infra*. This paper does not advocate that the FCA serve as an escrow agent in the context of any key-related functions. See also Section V.A.2.i. ("Management of Keys and Keying Materials"), *infra*. Concerning Clipper liability, consider the position of the U.S. Council for International Business:

Since Clipper is a hardware-based device through which information is encrypted, a compromise of the key will destroy the security of the system and all data contained therein. It is unclear how a company would know if the key has been compromised, who is liable, and who should bear the cost of replacement. Moreover, the consequential damages resulting from a breach in security might be tremendous and possibly unrecoverable. In DES and RSA systems, the user selects his own key; therefore, the keys are not susceptible to being compromised beyond the user's own control. In the case of Clipper, the main keys are assigned during manufacturing, are not changeable by the user and are escrowed with designated agencies. Even though the Government is responsible for developing and holding, or having access to, the keys, it has stated that it would not be liable for any compromise of the keys.

**-Federal Certification Authority ("FCA"):** In this Report, the expression FCA is taken to include all of the various functions of a federal certification infrastructure, which would include any policy registration authorities, policy certification authorities and subordinate certification authorities which are operated by, or on behalf of, the federal government.<sup>11</sup> When a particular component of the FCA is intended to be addressed (to the exclusion of other FCA components), that entity will be specified accordingly.<sup>12</sup>

---

*Business Views on Encryption and "Clipper" Before the U.S. Senate Comm. on the Judiciary, Subcomm. on Technology and the Law* (May 3, 1994) (statement of the USCIB). See Markoff, *Flaw Discovered in Federal Plan for Wiretapping*, N.Y. TIMES, June 2, 1994, at A1; cf. Stewart A. Baker, *Don't Worry Be Happy*, WIRED, June 1994, at 100 (stating that certain opponents to Clipper represents "the long-delayed revenge of people who couldn't go to Woodstock because they had too much trig homework."). Finally, the Clipper debate has been called "the first holy war of the information highway." S. Levy, *Battle of the Clipper Chip*, N.Y. TIMES MAGAZINE, June 12, 1994, at 46.

<sup>11</sup> The term Certificate Management Authority has been proposed by MITRE, and appears largely to describe the same functions and entities as the FCA. See MITRE, PUBLIC KEY INFRASTRUCTURE STUDY (April, 1994) [hereinafter MITRE STUDY].

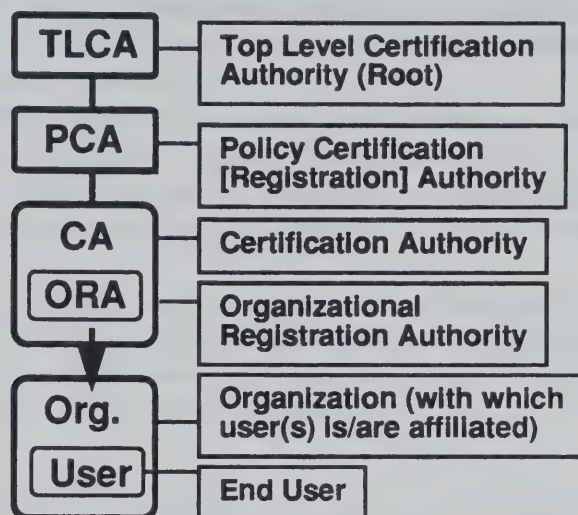
<sup>12</sup> The MITRE STUDY, *supra* note 11, employs the terms Policy Approving Authority ("PAA"), Policy Creation/Certification Authority ("PCA"), Certification Authority ("CA") and Certificate Management Authority ("CMA"). This Report will largely do so as well. PCA policies are specifically considered and compared in Section IX.C. and Appendix E, *infra*. Note that the TLCA is called a Policy Approving Authority in the MITRE Study; and the Organizational Registration Authority ("ORA") is called a Local Registration Agent within ANSI X9.30. Also, the United States Postal Service ("USPS") has tentatively adopted the term PCA to mean "Postal Certification Authority."

*Ed.-* An effort should be made to review, and to use where appropriate, pre-existing domestic, foreign and international terms in order to achieve the greatest possible degree of consistency. See text accompanying note 4, *supra*. The following terms are widely used in the public key community and are adopted for use in this paper as well:



**-Non-Repudiation:** "[P]rovides proof of the origin or delivery of data in order to protect the sender against the false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent."<sup>13</sup> However, only a trial of fact (made by a

---



<sup>13</sup> Introduction, *Working Draft Non-Repudiation Framework*, ISO/IEC JTC1/SC21, Project 97.21.9 Q53 (1989). Non-repudiation can be viewed as a component of dispute resolution by a trusted third party. From another perspective, non-repudiation is intended to provide proof sufficient to resolve one or more of the following disputes:

- The sender claims to have sent
  - a message, and the recipient claims not to have received it.
  - no message, but the recipient claims to have received it.
  - a message different than what the recipient claims to have received.
- The recipient claims to have received
  - a message but the sender claims not to have sent one.
  - no message, and the sender claims to have sent one.
  - a message different than what the sender claims to have sent.

In each of these cases, either the sender is a liar, the recipient is a liar, the computer and communications systems have created an error, or an interloper has caused a "spoof." Interview with Dario Tarentelli, Directeur, Veridial, in Paris (Oct. 26, 1992). See generally W. Ford, *COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES* 199-214 (1994). (considering "five distinct phases" of the nonrepudiation process: "service request, evidence

human being with the authority to resolve disputes) can provide ultimate non-repudiation. Consequently, the FCA would only provide proof to *support* non-repudiation, rather than non-repudiation itself.

**-Notary; Notary Public; Notarization:** A commissioned officer of a governmental entity that memorializes acknowledgments and performs other legislatively mandated acts.<sup>14</sup> Notarization in this sense does *not* include time/date stamping by persons not holding the title of notary public or by so-called *trusted devices*.

**-Trading Partners:** Governmental and private entities (including individuals) who are end-users of FCA services. The term *trading partners* is not limited to users of electronic data interchange mechanisms, nor to any particular type of information service or communication mechanism.

**-Trusted Third Party:** In general, "an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers."<sup>15</sup> Yet, certain important aspects of this definition require clarification in every new setting. For example, by whom must the

---

generation, evidence transfer/storage, evidence verification and dispute resolution").

Additionally, it has been noted that "a message has a semantic context in which it is interpreted and a big part of that context involves the time at which a message was sent and received. Without some form of (trusted) time stamping, non-repudiation is not a meaningful concept." Memo from Stephen Kent, Chief Scientist, BBN, to Michael Baum (July 10, 1993).

Another commentator has urged that each sender/signer can add its own time stamp -- it is the recipient's responsibility to independently determine whether to "accept" such time stamp. However, trusted time stamping is necessary to handle situations where a user revokes his keys in open systems. In more restricted systems, you can choose other solutions. See Memo from Peter Landrock, President, Cryptomathic, to Michael Baum (Apr. 27, 1994).

<sup>14</sup> See Section VIII.D. (Notaries Public), *infra*. Time stamping is considered in LINKING SECURITY, *supra* note 2, § II.e., at 44-45 and Sections V.A.2.b., V.C.4.f., V.D.7.b., *infra*. See also P. Anderson, *Foiling the Forgers*, DISCOVER, Oct. 1992, at 44, 163 (concerning the digital time stamping technology of Haber and Stornetta (of Surety Technologies, Inc.)).

<sup>15</sup> Baum, *Trusted Entity Debate Needs User Participation*, NETWORK WORLD, May 3, 1993, at 32.



Trusted Third Party be trusted: users, third party beneficiaries,<sup>16</sup> the FCA, or the entity responsible for dispute resolution? Also, what specifically is the trusted entity entrusted to perform and how will its trustworthiness be ensured?

- Vouch:** Frequently used in certificate-based public key cryptography standards documents,<sup>17</sup> this term is intended to convey the provision of evidence of the *binding* between an entity and its public key certificate. It is not intended to convey the provision of insurance, guaranties, or warranties, unless otherwise expressly indicated.

---

<sup>16</sup> See LINKING SECURITY, *supra* note 2, § III.b. & tbl. 5, at 54 (considering trust issues in the context of determining the primary beneficiaries of security). Also, consider the limitations on the protections available to third-party beneficiaries with respect to FCA acts and the extent to which such protections must be consistent with the *doctrine of insurable interest*, which "requires that there be some significant relationship between the insured and the person, the object, or the activity that is the subject of an insurance transaction." R. KEETON & A. WIDISS, INSURANCE LAW § 3.1, at 135 (Student ed. 1988).

<sup>17</sup> See, e.g., PEM Requests For Comment (RFCs)/Internet Standards; ANSI X9.30, *supra* note 5.

## IV. ASSUMPTIONS

The analysis of FCA liability depends upon many factors. This Report makes the following assumptions respecting certain of those factors.

**A. Organizational Status of the FCA** - Because the organizational status of the FCA remains unresolved, this Report's analysis encompasses a diverse range of possible organizational structures, including various combinations of federal government, quasi-government, and private entities. It should be noted that private law may not be applicable to the FCA because of sovereign immunity, federal pre-emption or the like. The absence of comprehensive FCA legislation is also assumed.

**B. Relationship Among CA Users**- It is assumed that FCA users intend to operate at *arms-length* and that they do not trust one another. While many trading partner and intra-governmental communications are undertaken in an atmosphere of trust, this Report assumes that protections at least as secure as those provided between highly competitive, hard-bargaining commercial entities will be required by the FCA. It is also assumed that the FCA will interoperate with commercial CAs to satisfy the requirements of a diverse range of commercial and private purposes (as well as, of course, government requirements).

**C. Information Requirements** - It is assumed that the FCA will utilize practices, procedures and technologies sufficiently strong to satisfy the anticipated legal requirements for the creation, communication, processing, retention, retrieval and deletion of a diverse range of government-related information, including information that satisfies, where necessary, both civil and criminal proof requirements. Such information would include, without limitation:

- a. non-classified but sensitive government documents<sup>18</sup>
- b. government procurement-related documents<sup>19</sup>

---

<sup>18</sup> Examples would be those compliant with the Computer Security Act of 1987 (codified at 40 U.S.C. § 759 note), 15 U.S.C. §§ 272 *et seq.*

<sup>19</sup> Examples would be those in compliance with the Federal Acquisition Regulation ("FAR"), 48 C.F.R. §§ 1.000 *et seq.* President Clinton, stated in a memorandum regarding "[s]trengthening [p]rocurement [t]hrough [e]lectronic [c]ommerce": "I am committed to fundamentally altering and improving the way the Federal Government buys goods and services by ensuring that electronic commerce is implemented for appropriate Federal purchases as quickly as possible . . . [and] by January 1997, complete Government-wide implementation of

- c. tax and treasury information requirements<sup>20</sup>
- d. health care insurance eligibility, treatment and claims materials<sup>21</sup>
- e. judicial pleadings, warrants, etc.<sup>22</sup>
- f. electronic government filings and record keeping<sup>23</sup>

---

electronic commerce for appropriate Federal purchases, to the maximum extent possible." Memorandum from President Bill Clinton to the Heads of Executive Departments and Agencies (Oct. 16, 1993).

<sup>20</sup> Examples would be those compliant with Internal Revenue Service, Federal Reserve, and Securities and Exchange Commission requirements. In contemplating the security infrastructure necessary to support tax and treasury requirements, consider that

[o]fficials say the electronic filing system is coming under increasingly bold and sophisticated attack. More than 25,000 fraudulent electronic returns were detected in the first 10 months of 1993, more than double the number in the corresponding period in 1992, as electronic filing grew last year to account for about 40 percent of all detected frauds. . . . Last year electronic filing accounted for 12 million returns, or slightly more than 10 percent, a figure the agency is counting on to rise to 80 million, or about two-thirds, by 2001. . . . The I.R.S. estimates its loss from electronic fraud alone at tens of millions of dollars a year, but it and outside specialists fear it could be much higher.

Hershey, *I.R.S. Finds Fraud Grows As More File by Computer*, N.Y. TIMES, Feb. 21, 1994, at 1A.

<sup>21</sup> Examples would be those compliant with Health and Human Services (HHS), Health Care Financing Agency (HCFA), Food and Drug Administration (FDA) and Drug Enforcement Agency (DEA) laws and regulations. Cf. 21 C.F.R. § 1306.05(a), promulgated pursuant to the Controlled Substance Act, 84 STAT. 1242 (1970) (codified at 21 U.S.C. §§ 801 *et seq.*) ("Where an oral order is not permitted, prescriptions shall be written with ink or indelible pencil or typewriter and shall be manually signed by the practitioner.").

<sup>22</sup> Examples would be those compliant with applicable federal and state evidentiary and procedural rules.

<sup>23</sup> Examples would be those compliant with National Archives and Records Administration, OMB and discrete requirements contained in regulations of diverse federal electronic filing initiatives. See generally Information Infrastructure Task Force, *The National Information Infrastructure: Agenda For Action* (Sept. 15, 1993); NIST, *Putting the Information Infrastructure to Work: A Report of the Information Infrastructure Task Force Committee on Applications*



- g. commerce in goods and services<sup>24</sup>
- h. financial instruments and payments<sup>25</sup>
- i. real property-related documents<sup>26</sup>

This means that the strength of the security provided by the FCA must be at least on par with the security needed to support "typical" business transactions. The strength of security necessary to support these requirements may necessarily increase the over-all stringency of (and burdens associated with) the binding process.<sup>27</sup> Because of the constraints imposed by the next

---

*and Technology*, Special Pub. 857 (May 1994) [hereinafter COMMITTEE ON APPLICATIONS].

<sup>24</sup> Examples would be those compliant with the Uniform Commercial Code (U.C.C.) and the United Nations Convention on the International Sale of Goods (Vienna, 1980).

<sup>25</sup> Examples would be those compliant with U.C.C. Art. 4A, the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Int'l Credit Transfers (1992) and the rules of various funds transfer systems.

<sup>26</sup> Examples would be those compliant with laws requiring that transfers of interest in real property be in writing. Note that the use of FCA services for the transfer of negotiable documents of title is not included in this list because "the creation of negotiable documents of title is a prerogative reserved solely for statutory law." B. Kozolchyk, *Evolution and Present State of the Ocean Bill of Lading from a Banking Law Perspective*, 23 J. MAR. L. & COM. 161, 240 (1992); see Sections VIII.G.4. through 6. *infra* (concerning documents of title). However, the FCA could be indispensable in support of computer-based title registries and other relevant mechanisms.

In addition to the types of information listed above, another categorization (for an "advanced National Information Infrastructure") proposes support for the following activities: electronic funds transfer, government regulatory data interchanges, collaborative engineering, enterprise integration and computer-supported collaborative work. COMMITTEE ON APPLICATIONS, *supra* note 23, at 26.

<sup>27</sup> See LINKING SECURITY, *supra* note 2, § III, at 45 *et seq.* (concerning risk-based approaches to security requirements). Consider the implications of doing so with respect to the possible future infrastructure being considered by the European Commission. Roland Hüber has remarked that "people are using low assurances/PGP [Pretty Good Privacy] and are willing to take risks -- more risks than we expect. [Consequently, we need to] focus on *general applications* needed by 'SMEs' [small and medium size companies]; and *low* assurances, not *no* assurances." Interview with Roland P. O. Hüber, Director, Advanced



assumption ("Availability"), it is assumed that the FCA will impose requirements on end-users that contribute to the satisfaction of the requirements below.

---

Communications Technology and Serv., Comm'n of the Eur. Community (CEC), in Brussels (June 18, 1993).

Responding to diverse information requirements, the U.S. Department of Defense established the following four "basic" policy statements:

1. DoD information systems must support information processing under multiple security policies of any complexity or type, including those for sensitive unclassified information and multiple categories of classified information.
2. DoD information systems must be sufficiently protected to allow distributed information processing (including distributed information system management) among multiple hosts on multiple networks in accordance with open system architectures.
3. DoD information systems must support information processing among users with different security attributes employing resources with varying degrees of authentication, data confidentiality, data integrity and access control.

DoD, Center for Information System Security, *Goal Security Architecture ES-3, -4* (Aug. 1, 1993). The Goal Security Architecture espouses a "fundamental security concept" that is relevant to the FCA: the *information domain* that is

defined as a set of users (or members), their information objects, and a security policy that dictates membership requirements and the protections needed for the information objects (rules for interdomain transfers are also part of the policy). A member of an information domain has the same access rights to all information objects in that domain; however, not all members have the same access rights. A single individual can be a member of more than one information domain; likewise, a single end system can support more than one information domain (assuming strict isolation).

*Id.* at ES-6. See NIST, *Computer Security Policy: Setting the Stage for Success*, CSL BULLETIN (Jan. 1994) (explaining computer security policy).

**D. Availability** - It is assumed that *availability* is to be provided by private data networks (*i.e.*, third party service providers ("TPSPs")), as distinguished from the FCA) in that TPSPs will facilitate communications between the FCA and other entities. Whereas, the services of authentication, integrity, confidentiality and non-repudiation are assumed to be provided only on an *end-to-end* basis. Also, with respect to security services, it is assumed that the preliminary implementation of the FCA will be on the provision of services in support of verifiable digital signatures (authentication, integrity and non-repudiation) rather than on confidentiality.<sup>28</sup>

**E. Support for Non-Repudiable, One-Time, Discrete Transactions** - It is assumed that the FCA's security and controls will be strong enough to support non-repudiable, one-time, discrete transactions between trading partners. Consequently, trading partners generally should not have to rely on a series of transactions or *customs and practices* (*e.g.*, a history of dealings and transactions) for proof purposes.

**F. Diverse Applications** - It is essential to consider FCA liability in the context of particular applications and legal regimes. For example, FCA liabilities relative to intra- or inter-governmental communications may vary from its liabilities relative to, say, maritime or sales transactions.

---

<sup>28</sup> Note, however, that this issue deserves further consideration, particularly to the extent that for FCA purposes, confidentiality and the referenced security services should not, and indeed cannot, be considered in isolation. Clearly, the national security requirements that necessitate controls on confidentiality must be balanced against the inherent requirements of a functional FCA. The draft position of the European Union on this issue states, "Expectations of confidentiality of electronic message services can currently not be met in the absence of international standards or internationally accepted methods. Uptake of these services by commercial users to support business processes will therefore have a natural limit, ie [sic] to those messages that someone usually writes on a postcard." COMMISSION OF THE EUR. COMMUNITY, GREEN BOOK ON THE SECURITY OF INFORMATION SYSTEMS, DRAFT 3.5 § 6.9.1, at 30 (June 5, 1993). "In practice we see no rationale nor need to relegate confidentiality to a hidden corner. You may have needs for signatures only, but in a large majority of cases you want to have some confidentiality as well, so that a separate scheme for the two does not make sense. This then has a significant impact on the options you consider both in organisation and approach." Email from R. Hüber, CEC, November 2, 1993.

The confidentiality requirements of the "MOSAIC" infrastucture also warrant consideration. *See infra* note 36. It is expected that the FCA infrastructure will support encryption keys in the future.



**G. Privilege, Not a Right** - It is assumed that the issuance of certificates to, and their possession by, users will be a *privilege* and not a *right*.<sup>29</sup> Evidence already exists that this assumption is in play. For example, although certificates are anticipated to become indispensable for conducting government, business and even private affairs and, as conventional methods are supplanted, the government does not at present intend to *require* individuals to utilize certificates in the proposed implementation. In addition, although the ability to make a holographic (handwritten) signature may be a strictly personal right beyond government intervention, digital signatures will necessarily substitute for holographic ones in "the digital world." Accordingly, the availability and use of certificates (and their supporting infrastructure) should not be considered indispensable during initial (limited and non-mandatory) FCA implementations.<sup>30</sup>

---

<sup>29</sup> The characterization in the text, it should be noted, does not eliminate the possibility of legal, as opposed to constitutional, rights arising in respect of the issuance and maintenance of certificates. Thus, users would presumably have a "legal right" not to be wrongly placed on a CRL, even though they might not have a "constitutional right" of due process prior to certificate revocation implicating principles of due process.

The right vs. privilege distinction raises constitutional issues which are discussed further in Sections V.B.3.e. and VII.A., *infra*. An interesting parallel to these issues concerns "universal service obligations" (by private or quasi-private entities) which are defined as "services that are supplied to customers or groups of customers at a loss, even when the firm supplying them is operating efficiently and its past investments have been based on sound business decisions." M. Cave, *et al.*, Meeting Universal Service Obligations in a Competitive Telecommunications Sector (Report to DG IV, CEC, Mar. 1994) at 1. (questioning the case for extending universal service obligations to *data services*..) *Id.* at 2.

Other issues with useful parallels to the FCA right vs. privilege question include the availability (whether cost-free or partially subsidized) of federal information resources; and the accessibility of the "data highway" to the poor. *See* OMB, Management of Federal Information Resources, Rev. Circular A-130, 58 Fed. Reg. 36,068 (Jul. 2, 1993); S. Katzen, Memorandum for Information Infrastructure Task Force (Jan. 24, 1994) (concerning the Government Information Locator Service (GILS)); Lohr, *Data Highway Ignoring Poor, Study Charges*, N.Y. TIMES, May 24, 1994, at A1 (concerning "electronic redlining"). These issues are largely beyond the scope of this paper.

<sup>30</sup> It has been suggested by European authorities that, because a name is a personal and inalienable right, naming authorities cannot *control* one's name, but may only *register* it. On this view, naming was urged to be a right and was thereby distinguished from a binding, which was urged to be a privilege. Interview with

**H. Consumer Transactions** - Because of the added complexity and risks typically imposed on providers of consumer products and services, this Report assumes that FCA-based transactions are undertaken among governmental units and "merchants."<sup>31</sup>

---

Roland P.O. Hüber, *supra* note 27. Although this "European view" is intuitively plausible, there are countervailing considerations. For example, government control over the naming of children is pervasive on the Continent. *See, e.g., What's In a Nom?*, *ECONOMIST*, July 31, 1993, at 46 (describing recent relaxation of naming restrictions in France). Similar laws exist in the Netherlands and Germany.

The author urges that the determination of whether a binding is a right or a privilege depends on the nature of the activity. When a binding becomes indispensable to the exercise of a right (*e.g.*, voting), it should also be viewed as a right. *See* *Shapiro v. Thompson*, 394 U.S. 618 (1969) (interstate travel); *Griswald v. Connecticut*, 381 U.S. 479 (1965) (procreation). And if FCA activities should become a right, relevant case law already exists concerning its enforcement. At least one court has held that the risk of erroneous deprivation of Medicaid benefits without human review of computer-based processes is unlawful. *See* *Tripp v. Coler*, 640 F. Supp. 848 (N.D. Ill. 1986).

With regard to "Distinguished Names" (DNs) "One's name may be one's own, but one's DN is a different matter. We are not born with DN's, we acquire them in the same way we acquire SSNs, telephone numbers, company ID cards, postal addresses, etc. Note that there is no DN form that is independent of one's organizational or geopolitical affiliation, i.e., every DN has built into it a name of an organization which with which you are affiliated or where you live. Since both of these characteristics change over time, it seems silly to make grandiose statements about the sanctity of one's DN." Memo from S. Kent to M. Baum (July 10, 1993) (on file with Independent Monitoring).

<sup>31</sup> *See* U.C.C. § 2-104 (defining "Merchant" to mean a "person who deals in goods of the kind or otherwise by his occupation holds himself out as having knowledge or skill peculiar to the practices or goods involved in the transaction, or to whom such knowledge or skill may be attributed by his employment of an agent or broker or other intermediary who by his occupation holds himself out as having such knowledge or skill"). "Merchant" status determines, *e.g.*, whether a warranty of merchantability is implied (U.C.C. § 2-314) as well as the existence and allocation of *good faith* obligations (U.C.C. § 2-103(1)(b)) and risk of loss (U.C.C. § 2-509).

Note that the proposed UNCITRAL "Draft Statutory Provisions" on the legal aspects of electronic data interchange (EDI) and related means of trade data



**I. Open Systems and Interconnected Networks** - It is assumed that the FCA must support the security needs of information in open systems and interconnected networks,<sup>32</sup> both domestically and internationally. It is further assumed that the FCA infrastructure should facilitate, and not create barriers to, international trade.<sup>33</sup>

---

communications, *see* U.N. Doc. A/CN.9/WG.IV/WP.57 (Aug. 9, 1993), will most likely not address "special issues relating to the protection of consumers." UNCITRAL, Report of the Working Group on Electronic Data Interchange (EDI) on the 25th sess. (Jan. 4-15, 1993), U.N. Doc. A/CN.9/373 9 (Mar. 1993), ¶ 29, at 8.

<sup>32</sup> *See* Robinson, *Internet's Business Degree*, INFORMATION WEEK, Aug. 30, 1993, at 17 (noting security as business' "primary concern" in Internet access); Markoff, *A New Information Mass Market*, N.Y. TIMES, Sept. 3, 1993, at D1 (quoting V. Cert in asserting that "[t]he Internet is now big enough that it qualifies as a mass market"). "Internet service providers are pressing the Securities and Exchange Commission to provide electronic access to the EDGAR electronic filing system through the Internet." Duffy, *Firms want Internet access to SEC's EDGAR*, NETWORK WORLD, July 9, 1993 at 12; *see* Markoff, *U.S. Shifts To a Freer Data Policy*, N.Y. TIMES, Oct. 22, 1993, at D1 (internet to carry S.E.C. corporate filings). *See also* Section VIII.H.1., *infra* (describing EDGAR). Consider that "[n]ew users of the Internet may fail to realize . . . that their sites could be at risk to threats such as intruders who use the Internet as a means for attacking systems and causing various forms of computer security incidents. . . . Such activity may be difficult to discover and correct, may be highly embarrassing to the organization, and can be very costly in terms of lost productivity and damage to data." NIST, *Connecting to the Internet: Security Considerations*, CSL Bulletin, July 1993, at 1. Open systems threats are considerable where passwords serve as the predominant security mechanism. "For the long term CERT [the Computer Emergency Response Team] suggests, network managers should reduce or eliminate the transmission of reusable passwords in clear text over the network." *How To Prevent Internet Rip-Offs*, INFORMATION WEEK, Feb. 21, 1994, at 20. "We're seeing automated attacks [by "sniffers" capturing passwords and monitoring traffic] involving thousands of hosts." Messmer, *Group warns of growing security woes on Internet*, INFORMATION WEEK, Mar. 28, 1994, at 9 (quoting Dain Gary, Manager of CERT). "Of the almost 200 computer crimes the FBI is investigating, 80% are related to the Internet." J. Panettieri, *Guardian of the NET*, INFORMATION WEEK, May 23, 1994, at 30, 36.

<sup>33</sup> *See generally* Kapor, *Where is the Digital Highway Really Heading?*, WIRED, July/Aug. 1993, at 53; Johnson, *NREN: Turning the Clock Ahead on Tomorrow's Networks*, DATA COMM., Sept. 1992, at 43.

**J. Government Consent to Be Liable** - It is assumed as a matter of policy that the federal government does not necessarily desire total immunity from liability for FCA activities. Rather, this Report considers various options for apportioning liability and presents differing degrees of liability ranging from total immunity to significant liability (including consequential damages).

**K. International Root Authorities** - It is assumed that no foreign or international CA, PCA or other registration authority will control the policies, operations, or liabilities associated with the FCA.<sup>34</sup> Foreign or international authorities will cross-certify.<sup>35</sup> International authorities, (e.g., name registration or standards-making organizations) are assumed to have no significant legal impact on FCA liability.

**L. Use of Card Technologies** - It is assumed that one or more card technologies, or *signature tokens*,<sup>36</sup> will be used to bolster the binding between each FCA user and his/her private key for all transactions of considerable value or risk.<sup>37</sup>

---

<sup>34</sup> This assumption recognizes the current difficulties associated with this matter, as demonstrated by the following comment:

It is evident there is going to be a fight. Between, on the one hand, the Internet Society and, on the other hand, those very other pretenders to the crown of acting as the US ADMD [Administrative Management Domain] - in place of this role once so proudly expected of now not-so-mighty Telecom operators. [We are] confronted by 1) the fact that the big agencies are vying for their part, that none will let the others do it, and they will certainly not let an outsider like the IS get involved; though they may agree and allow a "harmless" independent like the USPS! NO? (Of course they will each also run their own PRMD [Private Management Domain] CAs for internal assurance reasons, anyway, over and above any national infrastructure). Shrewd politiking [sic] is what I saw . . . !

P. Williams, E-mail List (Dec. 18, 1992).

<sup>35</sup> The Internet Policy Registration Authority (IPRA) could potentially be certified under an international organization, such as the International Telecommunications Union. See Section VII.A. ("International Organizations Generally"), *infra*. However, because the IPRA purports to be quasi-international in character and because there is perhaps currently no international organization presently with the prestige and capability of doing so, this issue requires further consideration. See Section VIII.G.2., *infra*.

<sup>36</sup> This term was proffered by Dr. Dennis Branstad of NIST in conversation with the author in May, 1993. Signature tokens may include integrated circuit (IC)



---

cards, smart cards, "smart diskettes," and PCMCIA (Personal Computer Memory Card Industry Association) cards. The reasons to consider such tokens continue to expand. *See, e.g., PCMCIA Prices Slipping*, DATAMATION, Nov. 15, 1993, at 15 ("Prices for credit-card size [PCMCIA] fax/data modems are beginning an expected steep tumble.").

Also, consider the increased availability of (and the government's trend towards permissive, if not mandatory, use of) hardware-based encryption in some environments. For example, the MOSAIC program will utilize a PCMCIA version 2.0 compliant TESSERA Crypto Card (encompassing requirements for the NSA's Multilevel Information System Security Initiative (MISSI)), which "will address the most prevalent needs for security in Automated Information Systems, including secure e-mail, digital signatures, electronic data interchange (EDI), file transfers, remote database access, and secure file storage and retrieval." NSA, MOSAIC OVERVIEW (1993). Also, note the extensive utilization of card technologies for various financial management and government electronic benefit transfers ("EBT") purposes. *See* Sections VIII.A.7. (considering EBT issues affecting card technologies) and A.2.i., *infra* (concerning the use of card technologies).

<sup>37</sup> For many applications, magnetic stripe cards are probably inadequate: "The encoding medium is visible, the codes themselves can be read using a teaspoon of powdered iron, the card can be re-coded using a machine available for \$2,500 from any of a dozen companies, and the encoding specifications are available in any good technical library." D. Bowers, *Identification cards are more than just security cards*, AUTOMATIC I.D. NEWS, Apr. 1993, at 28.

Recent events have exposed such weaknesses and bolstered the importance of more secure, or chip-based "smart cards." For example, *see* Johnson, *One Less Thing to Believe In: High-Tech Fraud at an ATM*, N.Y. TIMES, May 13, 1993, at A1 (reporting on the fraudulent recording of PINs entered by "hundreds of customers in their vain attempts to make the [illicit] machine dispense cash"); *see also* ATM: *A Tricky Move*, INFOSECURITY NEWS, July/Aug. 1993 at 10. However, issues remain concerning cost and flexibility of "hardware solutions."

Consider the potential influence (if any) on the use of smart card technologies as a result of the Comptroller General of the United States' DECISION B-245714, MATTER OF: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY -- USE OF ELECTRONIC DATA INTERCHANGE TECHNOLOGY TO CREATE VALID OBLIGATIONS (Dec. 13, 1991) ("The code or the digital signature evidences that intention [to contract], as would a handwritten or other form of signature. Both, generated using the sender's private key, are unique to the sender; and, the sender controls access to and use of his 'smart card,' where his key is stored.").

## V. SURVEY OF FCA ACTIVITIES CREATING LIABILITY EXPOSURE

Articulation of the scope and nature of anticipated FCA activities is critical to comprehension of their liability implications. This section identifies FCA activities, responsibilities and services that present potential liability,<sup>38</sup> and is intended to assist in an understanding of the nature and extent of various risks so that their systematic assessment and control may proceed. The categories of activities appear in roughly the order in which they would be undertaken within their life-cycle and are divided among four groups: FCA Organization and Roles, Certificate Application, Certificate Generation,<sup>39</sup> and Certificate Revocation. To provide context, activities implicating risk are presented along with aspects of the FCA that do not themselves constitute nodes of risk.

The absence of even preliminary decisions regarding the FCA's organization and functions and the nature of the law generally could produce an endless dissertation.<sup>40</sup> Recognizing the importance of making this survey an accessible and useful resource for future FCA development, the discussion of each topic herein is purposefully kept brief. Topics are briefly defined or described where necessary. Annotations provide reference to other sections in this Report and to other materials where specified issues are discussed in greater detail.

Editorial Note: Readers who are familiar with the technical aspects of certificate-based public key cryptography can pass over the remainder of this Section V without considerable loss of context. However, it is recommended, at a minimum, that the reader briefly scan the introductory paragraphs for each of its major subsections. Section V serves as a useful reference source and *check list*.

---

<sup>38</sup> The roles of PCAs, CAs and other authorities are consolidated for purposes of this survey. See Section III (defining the FCA to include these entities), *supra*.

<sup>39</sup> This category includes the operational use of certificates.

<sup>40</sup> It was casually remarked in contemplating a day of standards development activity on the ANSI X9.30 standard that "I am not sure whether the issues [in certificate-based public key] are like a stone rolling down a mountain which gets smaller and smaller as the stone chips are cut from the stone, or whether the better analogy is a snow ball rolling down a mountain which just keeps getting bigger!" Remarks of J. Stapleton, MasterCard, in Boston (July 22, 1993).



## A. FCA ORGANIZATION AND ROLES

### **A.1. Primary Roles of the FCA**

The FCA can potentially have many roles and provide diverse services.<sup>41</sup> Sections V.A.1 and V.A.2 herein constitute only one proposed division of *primary* and *secondary* roles and services. As a general principle, the more discretionary the FCA's roles and services, the greater its risks of liability. This distinction has been loosely characterized by certain policy and standards developers as the difference between (merely) *registering* users and *certifying* users -- the former being understood to represent a purely ministerial act and the latter being understood to implicate warranties or other assurances.

**a. Policy and Procedures Creation, Registration, Enforcement<sup>42</sup>**

**b. Certificate Creation,<sup>43</sup> CRL Creation<sup>44</sup> and Distribution**

**c. Accreditation and Certification:<sup>45</sup>**

---

<sup>41</sup> See ELECTRONIC CONTRACTING, *supra* note 2, ch. 5, reprinted herein as Appendix B) (considering *clearing houses*).

<sup>42</sup> Depending upon the policy in force, policy enforcement may range from providing a dispute resolution mechanism to simply taking action to terminate (via a CRL) a user's certificate. See *infra* Appendix E. The lack of treatment of enforcement issues in such policies should be noted.

<sup>43</sup> The CA might function as a clearing house for certificate requests originating from user applicants; in such a capacity it would bear responsibly for user certificate authentication and integrity.

<sup>44</sup> See Section V.D., *infra*.

<sup>45</sup> Here, certification concerns criteria (including standards), evaluation, testing and approvals that provide assurances of the FCA's trustworthiness, and of messages communicated thereunder. See *generally* Section IX.A. ("Certification and Accreditation"), *infra*. Also, issues concerning quality of service, safety and security must be tied to a particular standard of care. In the law, standards of care can range, *e.g.*, from *ordinary care* to *strict liability*. Cf. Section IX.D.2.a., *infra* at Table 9 (comparing standards of care for security). Additionally, presumptions associated with security may be established. See LINKING SECURITY, *supra* note 2, § IV, at 59-63; UNCITRAL, Report of the Working Group on Electronic Data Interchange on the work of its 27th sess. (U.N. Doc. A/CN.9/390) (Apr. 12, 1994), ¶¶ 139-143, at 33.

Of Users and Entities<sup>46</sup>  
Of Proposed Standards<sup>47</sup>  
Of Systems<sup>48</sup>  
Of Software  
Of Hardware<sup>49</sup>  
Of Other CAs

**d. Auditing<sup>50</sup>**

---

<sup>46</sup> This may include serving as an accrediter, a developer of curriculum, or an examiner for professional accreditation.

<sup>47</sup> E.g., this could involve setting parameters for the DSA's  $p$ ,  $q$  and  $y$  values, or the key sizes for RSA.

<sup>48</sup> This would be, for example, to the extent that systems are on an *approved list*. Also, consider the impact of certification based upon ISO 9000 Standard Series (Quality System and Registration) or a future rendition of GOSIP. Also, note that with respect to electronic filing of financing statements under U.C.C. Art. 9 ("Secured Transactions"), the Permanent Editorial Board (PEB) of the Commission on Uniform State Laws has recommended that a set of (undefined) minimum performance standards be used to determine whether a system is functioning satisfactorily and to provide a set of goals for reform. See PEB Study Group, U.C.C. ART. 9 REPORT, Dec. 1, 1992, at 89. See generally Section IX.A. ("Certification and Accreditation"), *infra*.

<sup>49</sup> Examples would be those consistent with NIST, FIPS 140-1 ("Security Requirements for Cryptographic Modules").

<sup>50</sup> Criteria and tools for auditing the FCA (e.g., control objectives and audit programs, respectively), as well as tools for assisting FCA users, need to be developed. Auditing/reporting criteria and tools should rigorously cover all FCA functions. Generally Accepted Auditing Standards (GAAS) should be available for FCA purposes. Cf. Generally Accepted System Security Principles ("GSSP") at note 1189, *infra*. Ad Hoc Panel on GSSP, *GSSP Draft Status & Initiatives*, 16th National Computer Security Conference (Sept. 22, 1993). GSSP were first proposed by the System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications of the National Research Council in its report *Computers at Risk* (1991), at 27. *Computers at Risk* noted that "a recognized standard for system design and development, which could consist of GSSP, can provide a yardstick against which liability can be assessed [or] it could inhibit innovation because of fears linking legal risks and the development of new products. GSSP could help allay such fears and curb capricious litigation by clarifying general expectations about what constitutes responsible design and development." *Id.* at 167.



- Auditing of FCA Entities (e.g., Root, PCAs and CAs)
- Auditing of Other Supporting Entities<sup>51</sup>
- Developing or Certifying of Audit Standards<sup>52</sup>
- e. Software, Hardware, or Service Developer

## **A.2. Secondary Roles of the FCA**

The following *secondary roles* of the FCA are generally understood to extend beyond the basic functions of a minimalist implementation, but the classification is not intended to suggest that the following services may not be indispensable to the practical and efficient operation of the FCA. To the extent that the FCA does not provide these *secondary services*, they will most likely be provided by private enterprise or other government entities. Many of the following services involve comparatively greater FCA discretion and, as noted above, commensurably greater risk.

- a. Communications (Voice and Data)<sup>53</sup>
- b. Time and Date Stamping  
Of Certificates<sup>54</sup>

---

<sup>51</sup> Other supporting entities may include those listed in Section V.A.1., *infra* (including third party service providers, banks, private users and notaries public). To the extent that such *Other Supporting Entities* include entities providing or using electronic data interchange, special audit requirements should be considered. See IIA, *Systems Auditability and Control* (1991); Mar *et al.*, UNDERSTANDING AND AUDITING EDI AND OPEN NETWORK CONTROLS (1991); Legal and Business Controls Task Group, ASC X12, *Model EDI Audit Program* (draft, April 1994).

<sup>52</sup> The need for specific audit standards for the FCA may dictate FCA involvement in the Federal Accounting Standards Advisory Board in making recommendations to the GAO, OMB and Treasury (or perhaps other applicable government entities) to ensure that accounting standards accommodate FCA activities. The Budget and Accounting Procedures Act of 1950, 31 U.S.C. § 3511(a), requires the Comptroller General, in consultation with the OMB and Treasury Department, to prescribe accounting standards for executive agencies.

<sup>53</sup> See Section VI.F.2. ("Defamation"), *infra*; see also Section VIII.B., *infra* (communications regulation and its impact on liability).

<sup>54</sup> There are various reasons for time stamping certificates, including the following:



Of Certificate Revocation Lists & Revocation Certificates<sup>55</sup>  
Of Messages

c. Directory Services<sup>56</sup>

d. Education and Training<sup>57</sup>

---

- a. To provide assurances of the time of creation of a certificate.
- b. To eliminate the need to retain the complete chain of certificates from the user to the Top Level Certification Authority (TLCA). Ostensibly the time stamping service would verify the complete chain of certificates, and the time stamped certificate would serve to verify that the certification path is valid/genuine. This procedure should be considered in the context of (i) record keeping requirements; (ii) requirements of trust (and perhaps accreditation); and (iii) notarial analogs to this procedure. *See* Section V.III.D. ("Notaries Public"), *infra*.
- c. To provide assurances of the time of revocation of a certificate.

<sup>55</sup> "Lists of revoked certificates are called Certificate Revocation Lists ('CRLs'). These contain time-stamped lists of certificates which have been revoked by a CA. Time-stamping is critical, to indicate the time at which the binding between an entity's public key and identity has been terminated. Upon revocation, the entity whose certificate is revoked cannot generate valid signatures with the private key corresponding to the public key on the revoked certificate." ANSI X9.30, *supra* note 5.

A revocation certificate "consists of the original certificate and additional information about the revocation such as date and reason of revocation, the date of known or suspected compromise, the party who requested the revocation, and the name of the CA who performed the revocation. The CA then signs the revocation information and thereby creates a self-contained revocation certificate. Such revocation certificates can be stored and handled in the same way as public key certificates are." TEDIS, FAST T1.1, *Credentials, Attributes and Certificates*, § 4.3, at 6 (March 31, 1994).

<sup>56</sup> This concerns both FCA-created/posted directory listings and FCA-operated directories. The ownership and control of directories is important to the integrity of directory data to the extent that any non-X.509 protected information is to be relied upon by the FCA and its users. *See* Section V.A.7.i. ("Directory Services and Related Data Bases"), *infra*.

<sup>57</sup> Note that federal agency obligations for "mandatory periodic training in computer security awareness and accepted computer security practice of all employees" is mandated by section 5 of the Computer Security Act of 1987, 101 Stat. 1727 (1988), *codified at* 40 U.S.C. § 759 note. *See* Circular A-130 Revised, 58

**e. Insurance<sup>58</sup>**

**f. Billing for Certificates, CRLs, etc.**

**g. Dispute Resolution Mechanisms;<sup>59</sup> Witness Services<sup>60</sup>**

**h. Key Generation<sup>61</sup>**

---

Fed. Reg. 36,070 (July 2, 1993) (concerning educational requirements); *see also* Section X.Q., *infra* (recommending that NIST "Promote and Integrate Audit, Legal and Security Education Extensively").

<sup>58</sup> It must be considered whether the provision of CA services constitutes a form of insurance and is thereby subject to the law and regulation of insurance. *Cf.* SEC v. Variable Annuity Life Ins. Co., 359 U.S. 65 (1959) (listing investment risk-taking, fixed return, guaranties that at least some fraction of the benefits will be payable in fixed amounts and true underwriting of risk as elements of insurance. There is also the question of whether the FCA will provide separate insurance (for a fee) comparable to that made available by the USPS to customers. *See* Section VII.A.4.a., *infra* (concerning the USPS); Section IX.B., *infra* (concerning insurance).

<sup>59</sup> Claims, demands, disputes, controversies and differences that arise concerning any term, condition, or provision of FCA policies or agreements might be settled in arbitration conducted by, and under the rules of, a designated entity, such as the American Arbitration Association. *See* Section IX.D.4. ("Alternative Dispute Resolution"), *infra*.

<sup>60</sup> Witness services might include providing expert testimony of CA practices in nonrepudiation disputes (whether or not they are related to FCA services), as well as of FCA-based *record keeper* services.

<sup>61</sup> Although the FCA should be *discouraged* from participating in private key generation or retention for others (for obvious liability and trustworthiness reasons), it is anticipated that some CAs will, for practical reasons, provide such services. It is not clear whether the CA would hold private keys in plaintext, or retain the private keys of others in any form whatsoever. In fact, the CA could benefit in ensuring that private keys (of others) are never retained under any circumstances.

If key generation services do not function within a trusted hardware environment (such as an environment incorporating the BBN Certificate Signing Unit/RSA Certificate Issuing System, smart cards, or other devices of comparable or greater strength) or do not utilize management controls (such as split authorization/secret sharing of the certificate generation unit's master keys), serious issues arise respecting the existence and strength of legal presumptions for



## i. Management of Keys and Keying Materials<sup>62</sup>

### Software- vs. Hardware-Based Key Storage and Access Controls Secret Sharing and Escrow<sup>63</sup>

### Use of Card Technologies<sup>64</sup>; Loss or Compromise of Keys

---

signatures by certified users of such keys. These issues are treated in context in LINKING SECURITY, *supra* note 2, § IV., at 63. tbl. 6.

<sup>62</sup> This role can also involve symmetric key management or the authenticated delivery of well-known keys. See ANSI X9.30, *supra* note 5, pt. 3.

<sup>63</sup> See generally Section VIII.C. ("Escrow and Other Legal Agents"), *infra*; NIST, *Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)*, 58 Fed. Reg. 40,791 (July 30, 1993).

*Secret sharing* can be defined as a system that distributes authorization in which two or more persons (who might function as escrow agents) are given a "piece of a secret" and all, or a subset of, such persons, depending upon the scheme/implementation must combine their respective pieces of the secret in order to activate or utilize a computer-based resource. The number of escrow agents that share the secret keying material should be susceptible to justification, but the author has not identified materials that provide a rigorously supported approach. Historically, the requisite number of persons has ranged from, *e.g.*, two for land-based nuclear weapons to more than 15 for the classified STU-III cipherphone master keys (according to one NSA employee). To borrow from military procedures, the "personnel reliability program" implemented for escrow holders might best be viewed as a "critical" rather than "controlled" duty assignment and therefore require commensurate investigation and controls. See Cotter, *Peacetime Operations*, in MANAGING NUCLEAR OPERATIONS 60-61 (A. Carter, *et al.* eds., 1987).

Note also that the EES does not establish the number of escrow agents and that in conversations with the NSA, it was represented that this matter was "fully delegated" to the Justice Department. "The escrow system may be indicated in some cases, in others it would not be acceptable and in many other cases it would be considered unnecessary. I also doubt that the operational experience from national security is applicable to the open environment of business and the general public." E-mail from R. Hüber, *supra* note 28.

<sup>64</sup> Card technologies include "smart cards," magnetic stripe cards, optical cards, and other technologies. The legal affect of using card technologies requires resolution of several issues, such as what presumptions should control the loss or compromise of keys. Also, the various purposes and functions that card technologies serve deserve rigorous legal review. A Westlaw search located no reported cases concerning "smart cards." Cf. COMPTROLLER GEN. OF THE U.S.,



**Protection of Communicated Keying Material**  
**Conventionally Communicated**  
**Electronically Communicated**

**A.3. Administration and Management**

The creation of the FCA's administration and management structure involves important decisions, most of which will affect the FCA's actual and perceived trustworthiness. As the following material demonstrates, many decisions address the roles and responsibilities of individuals. In this respect, the risks associated with the *human resources* aspects of FCA administration are potentially significant. One ongoing casual discussion among certification authority developers concerns, "How many and how much will it take to bribe the CA to issue a certificate or to disclose its private key?" Important implications derive from basic decisions concerning the strength and accountability of the FCA's management. As is true with most aspects of information security, a balancing of cost, benefit and risk is required. Given the extent of unknown risks at this early stage in certificate-based public key development, sound policy compels stronger, rather than weaker, management controls.

**a. Criteria for, and Oversight of, Upper-Level Management<sup>65</sup>**

---

DECISION B-245714 (Dec. 13, 1991), *supra* note 37 (mentioning smart cards but not cogently addressing their status). Additionally, case law addressing automated teller machine (ATM) card use and fraud is noteworthy but inadequately responds to the card technology needs of an FCA.

<sup>65</sup> The federal government has expressed the importance of upper level management in ensuring the integrity of diverse resources:

Financial Resources - "[A]n agency CFO must be a key figure in an agency's top management team." GAO, *The Chief Financial Officers Act: A Mandate for Federal Financial Management Reform* 6 (Sept. 1991). See generally Chief Financial Officers (CFO) Act of 1990, Pub. L. 101-576, 104 Stat. 2838 (1990) (codified in various provisions of 31 U.S.C.). To the extent that the organizational form and situs of the FCA remain uncertain, and that government corporations remain candidates for FCA implementation, the CFO Act is relevant. The CFO Act is applicable to government corporations and requires the submission of annual management reports and annual audits by the inspector general or an independent public accountant. See *id.*

Information Resources - "The head of each agency shall . . . have primary responsibility for managing agency information resources." Circular A-130 Revised, 58 Fed. Reg. 36,070 (July 2, 1993).

## **b. Criteria for, and Oversight of, FCA Employees<sup>66</sup>**

---

Note also that "The National Bureau of Standards [renamed NIST] shall . . . have responsibility within the Federal Government for developing . . . *management* . . . standards and guidelines." Computer Security Act of 1987, *supra* note 18, § 3 (emphasis added).

<sup>66</sup> Mismanagement by FCA employees can cause diverse problems and liabilities, including those resulting from private key compromise, inappropriate issuance of certificates, issuance of CRLs containing wrong certificate serial numbers and the disclosure of protected personal information. Consequently, the development of criteria for the selection and oversight of FCA employees requires close scrutiny. In this regard, consider (for FCA purposes) the scope of information required by the SEC's record keeping requirements with respect to partners, officers, directors, traders, managers, or any employee handling funds or securities, etc.:

A questionnaire or application for employment . . . shall contain at least the following information with respect to such a person:

- (a) His name, address, social security number, and the starting date of his employment or other association with the member, broker or dealer;
- (b) His date of birth;
- (c) A complete, consecutive statement of all his business connections for at least the preceding ten years, including whether the employment was part-time or full-time;
- (d) A record of any denial of membership or registration, and of any disciplinary action taken, or sanction imposed, upon him by any federal or state agency, or by any national securities exchange or national securities association, including any finding that he was a cause of any disciplinary action or had violated any law;
- (e) A record of any denial, suspension, expulsion or revocation of membership or registration of any member, broker or dealer with which he was associated in any capacity when such action was taken;
- (f) A record of any permanent or temporary injunction entered against him or any member, broker or dealer with which he was associated in any capacity at the time such injunction was entered;
- (g) A record of any arrest or indictment for any felony, or any misdemeanor pertaining to securities, commodities, banking, insurance or real estate . . . fraud, false statements or omissions, wrongful taking of property or bribery, forgery, counterfeiting or extortion, and the disposition of the foregoing.
- (h) A record of any other name or names by which he has been known or which he has used . . . .



### c. Establishing Personal vs. Entity Liability<sup>67</sup>

### d. Inadequacies of Sanctions Against FCA Employees <sup>68</sup>

---

17 C.F.R. § 240.17a-3(a)(12i).

<sup>67</sup> The "personal vs. entity liability" question concerns the extent to which individuals employed by a company or government can be held accountable and assurances that they can be criminally prosecuted and convicted for their wrongdoings when the evidentiary trail relies upon digital signatures rather than conventionally signed documents.

Two of the issues associated with this matter concern "group certificates" and card technologies. A public key certificate representing a group of users (a "group certificate") would require sharing the corresponding private key among that group of users. Thus, signatures generated using that private key would not authenticate the specific originator of a message, but would instead authenticate only the group, thereby reducing individual accountability. Such sharing of a private key may also increase the likelihood of key compromise if it is distributed to and stored in multiple computers. Card technologies, such as smart cards, may bolster the assurances of personal (vs. only entity) accountability. *See generally* Section IV.L. ("Use of Card Technologies"), *infra*; Section VIII.A.7.b., *infra* (concerning EBT issues and card technologies).

<sup>68</sup> The integrity of FCA employees is critical to the perceived and actual trustworthiness of the FCA infrastructure. Both *carrot* and *stick* approaches to bolstering integrity should be used, because improper actions by FCA employees could potentially cause extreme injury. Unfortunately, the carrots and sticks available under current federal policies, practices and laws are either too weak or unclear. One ranking Treasury Department manager noted that "sanctions on Treasury people are pretty well unspecified for unclassified information," that "this is forcing open our kimono," and that this is "a dirty little secret."

Some computer security specialists would like to see strict and definitive liability rules for FCA employees. In interviews, federal managers and policy makers who oversee computer-based information security concurred with the following proposed principles:

- a. that FCA employees and managers must be held personally liable, both criminally and civilly, for any impropriety, and to a higher standard, than other federal employees and the public at large;
- b. that personal liability should extend to negligence; and
- c. that current criminal and civil laws are inadequate to provide adequate assurances of prosecution, conviction and judgment.



**e. Delegation<sup>69</sup>**

**Constitutional Limitations<sup>70</sup>**

**Providing FCA Services on Behalf of Non-FCA CAs**

**Providing CA Services by a Non-FCA Entity on Behalf of FCA**

**Technical Aspects<sup>71</sup>**

**f. Communities of Interest (COIs)<sup>72</sup>**

---

The interviewees suggested that the extent of personal liability of Certifying Officers who authorize payments under federal law should be considered in the process of developing an appropriate scheme for the FCA. Additionally, federal security managers claimed that the existing laws and regulations provide agencies with extensive responsibility and flexibility, and that this has resulted in inaction and confusion. Existing penal laws do not contemplate the range of responsibilities and risks associated with managing public key infrastructure. See Section VI.G. ("Criminal Liability"), *infra*.

<sup>69</sup> One technical definition provides that "[d]elegation is the process whereby a user in a distributed environment authorizes a system to access remote resources on his behalf." M. Gasser & E. McDermott, DEC, *An Architecture for Practical Delegation in a Distributed System*, IEEE (1990).

<sup>70</sup> See Section VII.A.1., *infra*.

<sup>71</sup> See ANSI ASC X9.45 "Enhanced Management Controls Using Attribute Certificates" (1994) (a new work item intended to provide an "attribute certificate" to enforce explicit delegation) [hereinafter ANSI X9.45] ; Gasser & McDermott, *supra* note 69; see also Section VIII.C., *infra* (concerning various forms of delegation).

<sup>72</sup> Issues have been raised concerning liabilities associated with an FCA infrastructure that certifies users with respect to their *community of interest* rather than with respect to the *organization* within which they are employed. One concern was the extent to which the certificates issued by communities of interest should require organizational sponsorship. Provided that communities of interest are operated in an accountable fashion, and with the same *entity status* as an organizationally oriented CA, there should be no substantive difference in liability associated with the two methods of certification. Consider the following remarks from two public key developers:

R. Ankney:

If CAs were structured around communities of interest, I would think the user DNs [Distinguished Names] would still be organization-based, so you could still determine

#### **A.4. Relationships Among the FCA and Other Parties**<sup>73</sup>

As a new and as yet undefined entity, the FCA's relationships with other parties require considerable advance consideration and articulation because

---

who someone worked for from their DN. However, the CA name would likely be totally independent of the organization, so the PEM rule about user names being subordinate to their CAs would no longer apply. *E.g.*,

User name: "C=US; O=ABC Co.; OU=Accts Payable; CN=John Smith"  
CA name: "C=US; O=Accts Payable CA"

J. Lowry:

Mike, you've discovered the origins of the religious war. . . . CA's don't assign DNs in real life, Directory Administrators do (domain management function). In PEM (lacking directories) the CA did double duty, assigning DNs and signing certificates.

The example above could still be parsed such that an assumption of membership could be applied. *E.g.*, it is likely that John Smith works at ABC Co. and also that the CA represents ABC Co. The problem arises when the CA really works for DEF Co., a fierce competitor of ABC Co., and the recipient of a message signed by this certificate (signed by CA DEF) acts with the belief that John Smith works for ABC or represents ABC.

I think the following will likely be the practice:

- 1) "big" organizations will have their own CA and members of that org[anization] will have subordinate names.
- 2) "other" organizations will subscribe to a "CA Service" where the fact that this is a service will be apparent from the CAs name:

*e.g.*, "C=US; O=AT&T; OU=Certificates'R'Us"

- 3) In all cases, end users must only rely upon the policy statement of the root. They must learn not to attribute 'apparent' affiliation within the name components.

E-mail excerpts (July, 1993).

<sup>73</sup> Legal relationships raise issues such as agency and independent contractor liability. Powers of delegation, and the existence, extent and enforceability of agreements, including warranties and limitations of remedies or liability, are also comprised. The FCA might also be impleaded in litigation arising from a dispute between end users.

the conventional analogs among currently available entities do not necessarily provide a sufficient basis for accurate extrapolation. Moreover, as a primary provider of security and trust, difficult, and not necessarily intuitive, decisions must be made concerning the quanta of security that are to be contributed by the FCA and other parties. To the extent that the FCA is recognized as a primary provider of security, there is a danger that presumptions as to the extent of such requisite contributions will be weighted toward FCA responsibility.

**a. Governmental Providers of FCA-Related Services<sup>74</sup>**

**b. Third Party Service Providers/VANs<sup>75</sup>**

**Service Bureaus**

**Banks and Financial Services<sup>76</sup>**

**Network Services**

**Information Services**

**Data Registries**

**c. Government Users<sup>77</sup>**

**d. Private Users**

**e. Non-FCA Certification Authorities and Hierarchies<sup>78</sup>**

**f. International Relationships<sup>79</sup>**

---

<sup>74</sup> This concerns the relationship between the FCA and other government entities providing security and ancillary services. Mechanisms of interaction among aspects of the federal government such as Interagency Memoranda of Understanding (MOUs), Executive Orders, statutes or regulations need to be evaluated for their relative effectiveness in apportioning responsibility and risk.

<sup>75</sup> See generally Sections VIII.B. ("Value Added Networks"), VIII.G.1. ("Regulation of United States Telecommunications"), and V.A.5. ("Communications"), *infra*.

<sup>76</sup> See generally Section VIII.A., *infra*.

<sup>77</sup> Among many issues, the extent to which a government user can use the FCA for personal purposes should be articulated.

<sup>78</sup> Relevant legal issues include cross-certification, privity, confidentiality and third party beneficiary status, all of which are discussed elsewhere in this Report.

<sup>79</sup> These issues include those relevant to transborder data flow, conflicts and choice of law, as well as the capacity to exert extraterritorial controls where necessary to provide requisite assurances, all of which are discussed elsewhere in this Report.



#### **A.5. Communications<sup>80</sup>**

Communications, in both conventional and electronic forms, are critical to the proper operation of the FCA. Such communications will likely use many media, including phone, electronic mail, electronic data interchange and file transfer, and exhibit varying degrees of trustworthiness.

Communications will be undertaken both unofficially and in conformity with the policies and agreements among the many parties to FCA activities. The FCA must make decisions concerning the scope, nature, security and legal effect of its communications. The communications issues identified immediately below must provide for diverse levels of satisfaction of various legal requirements for adequate disclosure/notice and for confidentiality. FCA policy development and promulgation may face legal challenges for a diverse range of procedural and substantive reasons, including inadequate notice, accommodation of private sector interests<sup>81</sup> and vagueness.

##### **a. Certificates and CRLs<sup>82</sup>**

##### **b. Notices<sup>83</sup>**

---

<sup>80</sup> Communications issues include private-public interface, such as commercialization issues associated with Internet access. *See* Section V.A.4.b. (concerning Third Party Service Providers), *supra*. *See generally* Sections VIII.B. ("Value Added Networks") and VIII.G.1. ("Regulation of Telecommunications Common Carriers"), *infra*.

<sup>81</sup> Examples include Small Business Administration requirements intended to prevent barriers to the participation of small businesses.

<sup>82</sup> *See* Sections V.B. and V.C. (concerning certificates) and Section V.D. (concerning CRLs), *infra*.

<sup>83</sup> Notice is important for FCA purposes, particularly with respect to certificate revocation. *See generally* Section V.D. ("Certificate Revocation"), *infra*. Precise meanings for *notice* and *notify* must be established. One possible requirement of *notice* should be the delivery of notification in a timely manner or within an explicit period of time. The legal articulation of "notice" for FCA purposes should include whether it should or must be communicated via computer-based mechanisms or by, *e.g.*, USPS Certified or Registered Mail (and whether a return receipt should be requested), or a recognized courier service. The time at which notice is effective should also be defined (*e.g.*, upon "receipt").

When notice is sent electronically, the extent to which the recipient must verify its authenticity and acknowledge receipt should be determined. Because the Internet does *not* support a "return receipt" or "message confirmation" service,

**c. Directory Information**

**d. Identity and Locality Information on Other FCA Entities**

**e. Policies Statements and Agreements<sup>84</sup>**

**f. Attribute Certificate-related Information<sup>85</sup>**

**A.6. Establishing FCA Expectations**

The expectations of users (including, perhaps, third party beneficiaries) concerning certificate and CRL strength and reliability go to the heart of the FCA's *raison d'être*. Until such time as certificate-based public key use develops custom, usage, and trade practices of legal significance, there

---

the sender of an electronic notice may only *request* an acknowledgment of receipt from the recipient. Each party has an underlying obligation to exercise due diligence in maintaining system availability for electronic notice receipt. If the notice's originator does not receive an acknowledgment of receipt within a specified period (*e.g.*, two business days from the time sent), then an alternative arrangement should be developed (*e.g.*, to communicate via conventional means such as USPS Certified or Registered Mail or recognized courier service). Cf. Section V.A.2.b., *supra* (notice concerning "revocation certificates"); Section V.C.3.a., *infra* ("Push versus Pull").

Also, the issue of which persons and entities are entitled to notice requires resolution (*e.g.*, need notice be given only to a representative of a group or to each member of a community of interest?). See Section X.L., *infra* (recommending resolution of disclosure, notification and warning mechanism issues).

<sup>84</sup> Policy statements and agreements are considered in Section IX.C., *infra*. See also Section X.D. (recommending that NIST "Develop FCA Agreements and Policies"), *infra*.

On the advisability of using standardized FCA policies, agreements and the like, an interesting parallel to insurance practices deserves consideration: "[S]tandardization has been required by state legislation as a means of implementing public policy. . . . That the use of standard insurance forms generally serves the interest of individual policyholders, the public, and insurance companies in having efficient and economical insurance operations appears to be a proposition beyond effective challenge." KEETON & WIDESS, *supra* note 16, § 2.8, at 120.

<sup>85</sup> See generally Section V.C.4. ("Attribute and Other Certificates"), *infra*. The requirements for the communication of Attribute Certificate information might be established by an "Attribute Authority" (AA). See ANSI X9.30, *supra* note 5, § 4.8, at 38.



remains a significant need to articulate FCA-related expectations expressly (e.g., in agreements, policy statements, etc.).

The following list identifies important areas where expectations can either be expressed, or which have particularly compelling requirements for expectational certainty. Ultimately, however, virtually all issues raised in this survey demand articulation of expectations.

**a. FCA Policy Development and Promulgation<sup>86</sup>**

**Notices and Advertisements<sup>87</sup>**

**Agreements, Legislation, Regulation<sup>88</sup>**

**Guidelines, Operational Materials and Procedure Manuals<sup>89</sup>**

---

<sup>86</sup> Standards of identity (strength of binding requirements) and the procedures that implement and enforce such standards affect the FCA certificate's strength and purpose, including the extent to which (i) publicized standards of identity are met by each subordinate CA, (ii) adequate assurance is provided that the FCA's keying material is protected, and (iii) certificates and CRL issuing policies are met and auditable.

<sup>87</sup> Users must be made aware of the differences in FCA policies so that they can make informed decisions as to the trustworthiness of the identity information contained in a certificate. It must be possible for any user to determine (unambiguously) the policy under which any certificate was issued. The means by which a user is alerted to these differences should be simple, uniform, and automated. The current (PEM) architecture achieves this through the use of PCAs, prohibition of cross-certification, and the requirement that PCA policies be available on-line. *See* S. Kent, *PEM WG Meeting Minutes* 6 (July 14, 1993); Section V.A.5.b., *supra* (concerning Notices). *See generally* Section IV (concerning advertising and its potential risks in the context of warranties and misrepresentation), *infra*.

<sup>88</sup> The choice of vehicles through which the FCA expresses its policy and procedures holds important implications affecting liability and political capital. A particularly telling example of initial regulatory proposal failure is demonstrated by the Federal Maritime Commission's proposed "Automated Tariff Filing and Information System User Agreement" to bind private users of FMC data resources. *See* Section VI.B.1., *infra* (describing the AFTI proposal and its legal problems).

<sup>89</sup> The FCA should adopt reasonable procedures in the form of a Certificate Management Procedures Manual ("Procedures Manual") or the like for the implementation and administration of its responsibilities. These procedures are necessary to ensure the security and confidentiality of private keys, certificates and other information. The Procedures Manual should be frequently reviewed and



## Certificates and CRL Content<sup>90</sup>

### b. Issuing Certificates:

#### To Subordinate CAs and Entities For Cross-certification<sup>91</sup>

---

updated. Each FCA entity and user should acknowledge that it has adopted, or will adopt and implement, the Procedures Manual prior to providing or using FCA-related services.

Procedures manuals might address level of service definitions, security and auditing standards, disclosure standards, and other issues raised in this section. See Section IX.C., *infra* (discussing many of the available CA policies in connection with the Internet PEM certification infrastructure); ANSI X9.30, *supra* note 5, app. B ("Alternative Trust Models").

<sup>90</sup> FCA expectations will likely be established, in part, within certificates and CRL content. For example, ANSI ASC X9.F1 has initiated a work item to provide for liability code indicators in certificates so that "[a]ttributes might be used to indicate security policy and assurance information for a particular CA. . . . Unless specified in separate agreement(s), the degree to which the CA has agreed to assume liability for the binding process and the security of the CA and its public/private keys shall be included in a 'LiabilityLimitation' attribute." ANSI X9.30, *supra* note 5, draft app. E (now moved to aforementioned new work item).

<sup>91</sup> Cross-certification is a process by which the scope of the certification hierarchy is extended. It permits a user holding the public component for one certifying authority to validate certificates issued by another certifying authority.

Among the issues arising with cross-certification is certainly the issue of what constitutes proper cross-certification. See Figure 4 ("Hypothetical FCA Legal Structures/Relationships"), *infra*. For example, suppose CA-1 registers with its TLCA a policy that purports to be a "medium strength/assurances" policy and CA-2 registers with its respective TLCA a policy that purports to be a "high strength/assurances" policy. Assuming that cross-certification should be undertaken only between entities which are, at a minimum, of comparable strength/assurances, on whom should we rely to decide whether CA-2's policy is sufficiently comparable to CA-1's policy so that expectations of trustworthiness of the cross-certification can be reasonably assured? It would be imprudent in this case, for example, for CA-2 to rely on CA-1's representations of security strength. Consider that some of the underpinnings of this scenario are exemplified by the proposed policy submitted by the COST International Consortium, see Appendix E.4., *infra*, which purports to be a "high-assurance" PCA. A related issue concerns whether it is both reasonable and practical to rely on a certification authority's (or its TLCA's) representations of trustworthiness. See generally Section IX.A.

**c. Hierarchical vs. Distributed Trust Models<sup>92</sup>**

**d. Availability (Denial of Service)<sup>93</sup>**

**Contingency/Disaster Planning and Recovery<sup>94</sup>**

---

("Accreditation and Certification"), *infra* (proposing mechanisms to ensure and enforce well-articulated and recognized levels of assurance).

Also, depending on the hierarchies, cross-certification can have other constraints. Consider the following with respect to PCA cross-certification:

Since PCAs do not have names that are distinguished in any way, if one PCA certifies another, the resulting certificate is syntactically indistinguishable from one that would be issued by a PCA certifying a CA. Yet another PCA certainly would not, in general, be expected to implement the same policies, so the semantic implications of PCA cross-certification would violate the model defined in [RFC] 1422. The result would leave users unable to determine the policy under which a certificate was issued, and the name subordination checking rule would have to be bypassed (or would often reject paths). So, PCA cross-certification, is not permitted under 1422 for a variety of good reasons."

S. Kent, E-mail List (July 30, 1993).

<sup>92</sup> In hierarchical trust models, administrative costs are higher and the loss is potentially greater upon private key loss or compromise. In distributed trust models, there is a longer verification chain (up or down), and a *chain of certificates* can provide leverage for the "up" path. FCA legal rules/guidelines will necessarily need to accommodate the specific trust model(s) incorporated -- generic rules/guidelines are anticipated to be inadequate.

<sup>93</sup> The property of being accessible and usable upon demand by an authorized entity. See International Standards Organization (ISO) 7498-2-1988(E). Transaction processing and just-in-time manufacturing are two examples of where availability has been demonstrated to be particularly critical. Directories (*e.g.*, for X.509 certificate look-up) and particularly CRLs are two critical areas demanding availability. Consequently, because the need and expectation of availability will depend upon the applications and environments, availability should be clearly articulated.

<sup>94</sup> Whether act of god/force majeure should exculpate the FCA from liability for unavailability requires decision. See MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, *supra* note 2, § 10.2(b), at 59 (providing for suspension, rather than default, "if the performance of a party . . . is delayed or prevented by an act of God, natural disaster, computer or communications failure or other cause beyond



**Re-Creating Government and User Records<sup>95</sup>**  
**Impact on Loss of Government Funds or Property**  
**Prevention of Malicious Software (Viruses, Worms, Etc.)**

---

the affected party's reasonable control"); *see also* ANSI X9.30, *supra* note 5 (discussing CA disaster recovery).

<sup>95</sup> The requirements for government archival of information in electronic form under the Federal Records Act (FRA) (codified at 44 U.S.C. §§ 2101 *et seq.*; 2901 *et seq.*; 3101 *et seq.*; 3301 *et seq.*) were reviewed in *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993) (mandating the archiving of information in electronic form and reiterating the FRA requirement that each agency head establish such safeguards against the removal or loss of federal records as he "determines to be necessary and required by regulations of the Archivist"). *See Lewis, Government Told to Save Messages Sent By Computer*, N.Y. TIMES, Aug. 14, 1993, at A1, A6.



#### **A.7. Intellectual Property Protections<sup>96</sup>; Privacy and Confidentiality<sup>97</sup>**

The intellectual property rights (including copyright, patent, and "hybrid" rights<sup>98</sup>) in FCA-related information and technology have yet to be

---

<sup>96</sup> This includes the treatment of copyright, patent and proprietary rights by the FCA, including domestic and international use, licensing, and royalties. The potential volume and variety of information collected, processed and retained by the FCA will be considerable. The use and ownership of such information is unresolved. A recent controversy concerning information resources within the Federal Maritime Commission (FMC) is illuminating.

The FMC's Automated Tariff Filing and Information System's proposed User Agreement (*see* Section VI.B.2., *infra*) raised data ownership issues that bear potential relevance to the FCA. For example, the proposed User Agreement stated that "all right, title and interest in ATFI data are and shall continue to be the exclusive property of FMC . . ." 58 Fed. Reg. 7501, 7505 (Feb. 8, 1993). One public comment filed in response to the proposed regulation stated that "[T]he commission's assertion of ownership exceeds its statutory authority, conflicts with other statutes, transgresses First Amendment principles, and distorts the relationship between citizens and their government." Comments of the Information Industry Association, *et al.* on Proposed Implementation of Section 502 of P.L. 102-582 (46 C.F.R. § 514), Mar. 10, 1993. Another comment noted that "the tariff data covered by the [User Agreement] is like a derivative work produced at the government's direction, and the license rights the Commission seeks to provide by contract are identical to the rights held by copyright owners." Comments of Transax Data, *id.* There are also issues concerning first amendment rights against restrictions on access to government information, *see, e.g.,* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 583 (1980) and diverse issues associated with the *secondary use* of such information.

<sup>97</sup> Consider, *e.g.,* that the "TIS-PCA [Trusted Information Systems - Policy Certification Authority] reserves the right to inspect the records of each CA authorized by TIS-PCA to check for compliance with the naming rule." Appendix E.5.3. hereto, at § 4. Privacy of a CA's users (particularly those which are not within the same organization) might be violated by a mandatory right to inspection procedure without appropriate limitations. Cf. the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 *et seq.*; National Telecommunications and Information Administration, *Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information; Notice*, 59 Fed. Reg. 6,842-49 (Feb. 11, 1994) (stating that "there are no federal statutes governing the secondary use of [telephone service and billing records]"). *Id.* at 6845.

<sup>98</sup> *See generally* Nimmer & Krauthaus, *Information as Property: Databases and Commercial Property*, 1 INT'L J. L. & INFO. TECH. 3 (1993).

articulated. The failure to delineate information rights rigorously creates considerable risks, particularly because the field of "information law" is a rapidly evolving one. Similarly, legal requirements concerning information privacy are being redefined in many areas, such as health care information management, the European Community's data protection initiative and the privacy implications of Clipper/Capstone. Moreover, because the disclosure of confidential or privacy-protected information is often precluded from contractual limitations on consequential damages,<sup>99</sup> these issues present considerable risks for the FCA.

**a. User Identification (Including Name) Information<sup>100</sup>**

**b. Algorithms<sup>101</sup>**

**c. Technical Specifications**

---

<sup>99</sup> For example, see MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, *supra* note 2, § 9.3 (permitting the optional exclusion of consequential damage limitations upon breach of the Model Agreement's confidentiality clause).

<sup>100</sup> Consider the remarks of Roland P. O. Hüber to the effect that "no one should be able to declare a [] name property." Interview with R. Hüber, *supra* note 27; cf. Greidinger v. Davis, 988 F.2d. 1344 (4th Cir. 1993) (overturning requirement of providing one's social security number for inclusion in a publicly available voter roster and noting Congressional recognition that "widespread use of SSNs as universal identifiers . . . 'is one of the most serious manifestations of privacy concerns in the Nation'" (quoting S. Rep. No. 1183, 93d Cong., 2d Sess. (1974)).

<sup>101</sup> This concerns the ownership and right to use algorithms as well as limitations on the adoption of patented technology in national and international standards. These issues, of course, have received the greatest publicity with respect to the patent status of public key algorithms. In this regard, see NIST, *Notice of Proposal for Grant of Exclusive Patent License*, 58 Fed. Reg. 32,105 (June 8, 1993) (notifying the public of NIST's intent to "grant an exclusive world-wide license to Public Key Partners of Sunnyvale, California to practice the Invention embodied in U.S. Patent Application No. 07/738.431 and entitled 'Digital Signature Algorithm'"); Messmer, *Gov't Backs Off on DSS Patent Battle*, NETWORK WORLD, July 19, 1993 at 9, 12 ("For the sake of getting on with the job, the government agreed to the cross-licensing scheme. . . . the underlying goal is to break the legal logjam." (quoting Lynn McNulty, Asso. Dir. for Computer Security, NIST)); M. Baum, *The Proposed Digital Signature Standard: Implications for Electronic Data Interchange*, 8 COMP. L. & SEC. REP. Issue 3 (Elsevier, Sept.-Oct. 1992).



- d. Certificates and CRLs<sup>102</sup>
- e. Public and Private Keys
- f. Digital Signatures<sup>103</sup>
- g. Standards<sup>104</sup>
- h. Hardware and Software
- i. Directory Services and Related Data Bases<sup>105</sup>

#### **A.8. Duty to Assist or Enforce**

The extent to which the FCA is obligated to assist either law enforcement personnel or non-FCA entities/users may affect FCA exposure. It also

---

<sup>102</sup> Cf. Section VIII.F., *infra* (noting that passports remain the property of the federal government). Attribute certificates that state delegated powers and other information of potential proprietary nature, as well as CRLs that contain "reason codes," may require confidential treatment. See Section V.D.6.f., *infra*.

<sup>103</sup> Issues have been raised as to whether the government can *own* a person's signature. See T. Jones, E-mail postings (May-June, 1993) (characterizing holographic and digital signatures as an inherent personal right). The imposition of a license fee "every time we sign something digitally amounts to the imposition of a general stamp tax." M. Seecof, E-mail posting (July 1993) (likening a license fee to "attempts by George III's government to impose various stamp taxes on American colonists"); see also Interview with R. Hüber, *supra* note 27.

<sup>104</sup> The ownership rights in standards, including the rights to republish, redistribute and obtain royalties from the sale of standards, has been a contentious issue in many standards organizations, including ANSI and IEEE. See ELECTRONIC CONTRACTING, *supra* note 2, § 6.13, at 448 (considering "whether standards for information exchange can be copyrighted"); § 8.16 at 451 ("Ownership of Property Interest in Standards"); § 8.18 at 454 ("Policies for Reprinting Standards").

<sup>105</sup> See *Telerate Systems, Inc. v. Caro*, 689 F. Supp. 221 (S.D.N.Y. 1988); cf. *Secure Servs. Technology, Inc. v. Time and Space Processing, Inc.*, 722 F. Supp. 1354 (E.D. Va. 1989); *Feist Publications v. Rural Tel. Services*, 499 U.S. 340 (1991); see also *Nimmer & Krauthaus*, *supra* note 98, at 24-25; R. Graham, *Directories: The Legal Issues*, 10 COMP. L. & SEC. REP. Issue 3 (Elsevier, May-June 1994) at 127-130 (concluding that the "lack of harmonization between EC member states' copyright protection for databases is correctly considered to be a serious hindrance to the free flow of information, such as use directories" and that "[s]ubscribers to, and providers of, directory services should consider carefully their potential losses arising from errors in the directories and seek suitable contractual and insurance protection."). *Id.* at 130.



requires coordination with other federal entities, such as the Justice and Treasury Departments, to ensure both that the respective departments are suitably accountable for their FCA-related duties and that investigative and prosecutorial services are sufficiently sophisticated to handle the novel and precedent-setting litigation that could well result from FCA activities.<sup>106</sup> To the extent that FCA management is apprised of these risks and fails to act, there is a potential for liability.<sup>107</sup>

**a. Investigations and Production of Evidence<sup>108</sup>**

**b. Criminal<sup>109</sup> and Civil Prosecution**

**c. Establishing Non-FCA Secure Environments<sup>110</sup>**

---

<sup>106</sup> This is not to suggest that the FCA will encounter significant litigation. Rather, it is simply gauged to reflect the experience of other government entities, particularly those offering services to the public, with respect to the quantity of litigation. The USPS is, perhaps, the best example of this phenomenon. *See* Section VII.A.4.a. ("United States Postal Service"), *infra*.

<sup>107</sup> *See generally* Section VII.A.3. ("Liability of the Federal Government Generally"), *infra*.

<sup>108</sup> As an historical aside, "[t]he sender or the addressee of a private telegram must prove his identity when requested to do so by the office of origin or the office of destination respectively." Telegraph Regulations, Ch. IV., Art. 7, amended to the Int'l Tele. Convention, Madrid 1932; *see* Section V.A.2.g. (proposing an FCA service to provide dispute resolution and witness services), *supra*.

<sup>109</sup> *See* Section VI.H. ("Criminal Liability"), *infra*.

<sup>110</sup> The duty to contribute to "Non-FCA Secure Environments" might include the sealing of trusted boxes (*e.g.*, time stamping devices) and participation in accreditation and certification activities. *See* Section IX.A. ("Certification and Accreditation"), *infra*.

### **A.9. Capitalization, Liquidity and Damages Fund**

In the event the FCA contemplates substantial liability, funds should be identified as to source and extent for the compensation of parties.

Particularly challenging issues that require resolution before such funding issues can be resolved include the quantitative determination of risks; the organizational structure's impact on FCA liability; and the need for, and availability of, insurance.<sup>111</sup>

- a. Sufficient Capitalization<sup>112</sup>**
- b. Legislative or Administrative Limitations**
- c. Commercial Insurance; Reinsurance**
- d. User, Member, or Agency Indemnification<sup>113</sup>**
- e. Risk Pools; Self-Insurance**

---

<sup>111</sup> See generally Section IX.B. ("Insurance"), *infra*.

<sup>112</sup> Sufficient capitalization is required for *responsible* private enterprise. Consider also the Clinton Administration's approach to the funding of the Clipper-Chip proposal, which utilizes confiscated funds and property, albeit subject to the constraint that the use of such funds be related to law enforcement. See the Adequacy of Appropriations Act, 41 U.S.C. § 11(a); Section VII.A.2. ("Authorization to Expend Funds"), *infra*.

<sup>113</sup> See Sections VII.B.1. ("Federal Contractor Liability"); Section VIII.C. ("Escrow and Other Legal Agents"), *infra*; see also Section IX.C. ("Policy Statements and Agreements") (concerning indemnification of CAs), *infra*.

## B. THE CERTIFICATE APPLICATION PROCESS<sup>114</sup>

### **B.1. Completeness & Propriety of Certification Request Data (CRD)**<sup>115</sup>

The completeness and propriety of CRD serve as a critical foundation for the issuance and use of FCA certificates. Certificate authenticity in the absence of extrinsic investigation and information can, at best, be no better than the CRD upon which the certificate issuance was based. The practical and legal limitations on required CRD, and the scope and manner in which CRD is submitted by individuals subordinate to their respective organizations (as well as nonhuman certificate applicants, *e.g.*, a trusted time stamping device), require resolution. The stringency of CRD requirements and related procedures affects the meaning and value of FCA-issued certificates, and therefore affects potential FCA liabilities.

#### **a. Applicant Identification Information Requirements**<sup>116</sup>

---

<sup>114</sup> This Section V.B. considers the creation and proper binding between certification request data (CRD) and the subject public key/certificate. Following the decision to issue a certificate, the generation of the certificate is considered in Section V.C. ("Certificate Generation"), *infra*.

<sup>115</sup> CRD "includes the [certificate applicant's] public key, entity identity and other information included in the certificate or otherwise used in the certificate management process." ANSI X.30, *supra* note 17, at 2. Concerning identity in an industry relevant to the FCA, the Bank for International Settlements has urged banks to "institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity." World Bank, Committee on Banking Regulations and Supervisory Practices, *Prevention of criminal use of the banking system for the purpose of money-laundering, Statement of Principles* (Basle, Dec. 1988).

<sup>116</sup> As an aside, attributes of inaccurate CRD can be analogized to those resulting from the submission of inaccurate information on an insurance application:

[If] the submission of incorrect information subsequently becomes the basis for the rejection of a claim for insurance benefit that then results in litigation, such an incorrect statement will be classified by a court as either a "warranty" or as a "representation," and the consequences of this classification -- which depend on (1) the circumstances, (2) the type of insurance involved, (3) the insurance contract terms, (4) the applicable legislative provisions, and (5) judicial precedents -- are of considerable significance to the rights of the parties. . . . More than one commentator has used characterizations such as "confused," "erroneous," "misleading," and "inconsistent" to describe the body of



---

law . . . that determines the rights of the parties to an insurance contract when it is subsequently discovered that an application for the insurance coverage contained incorrect information . . . .

An insurer is entitled to relief on the basis that an insured provided incorrect information in an insurance application, when it is proved (1) that the information was not correct, (2) that the information received was important either to the insurer's decision to insure or to the terms of the insurance contract (that is, the information was "material"), and (3) that the insurer in fact relied on the incorrect information.

KEETON & WIDISS, *supra* note 16, § 5.7, at 567-570.

Insurance law also provides an approach potentially relevant in determining when a user is obligated to notify the CA for CRL purposes, and the results of failing to do so: "A special type of concealment problem is presented as to whether an applicant is obligated to report either (1) a significant change in regard to information which was sought by the insured or (2) information that was unknown to the applicant when the application was filed, but which becomes known by the applicant after the application is filed." *Id.* at § 5.8(b). Keeton notes that there are "a range of judicial" views on this subject, but cites the New Jersey Superior Court as follows:

An insurance contract . . . requires the highest degree of good faith and fair dealing between the parties [and] requires the insured to advise the insurer of such matters that he knows might influence the insurer in entering into or declining the risk, at least where such facts are not of record and are not discoverable therefrom by the insurer.

*Id.* § 5.8, at 574-575.

Finally, Keeton notes that an applicant makes a "continuing representation" of the facts in the application until it is issued. The FCA should obligate its users to make comparable continuing representations. *Id.* § 5.8(b), at 575.

Among other remedies, the Program Fraud Civil Remedies Act of 1986, 31 U.S.C. § 3801 *et seq.*, provides:

- (a)(1) Any person who makes, presents, or submits, or causes to be made, presented, or submitted, a claim that the person knows or has reason to know—
  - (A) is false, fictitious, or fraudulent;
  - (B) includes or is supported by any written statement which asserts a material fact which is false, fictitious, or fraudulent;
  - (C) includes or is supported by any written statement that—
    - (i) omits a material fact;
    - (ii) is false, fictitious, or fraudulent as a result of such omission; and

## Quality of Identification Documents<sup>117</sup>

### Personal Presence<sup>118</sup>

---

(iii) is a statement in which the person making, presenting, or submitting such statement has a duty to include such material fact; or

(D) is for payment for the provision of property or services which the person has not provided as claimed,

shall be subject to, in addition to any other remedy that may be provided in law, a civil penalty . . . .

*Id.* § 3802.

<sup>117</sup> For an unsettling look at the ease with which one may obtain and use fraudulent identification, *see* HOW TO CREATE A NEW IDENTITY (1983). This book notes that it "not only . . . contain[s] information on how to become a new person, for whatever reasons, but also [on] how to erase your past completely." *Id.* at 2. The anonymous author continues:

What has always surprised me is how simple it is to establish valid United States documentation under an assumed name and how much people rely on that piece of plastic or paper that says "I am John Doe". . . . One of the reasons the use of valid documentation and an assumed name works so easily is that this is one of the few countries in the world that does not have one unique national document, easily scrutinized, to identify the bearer. Consequently, documents not initially intended to serve as standardized I.D. are used as such in every state. The advantages of this system to you are obvious.

*Id.* at 6; *see also* Section VIII.F., *infra* (concerning U.S. Passport identification requirements and procedures).

It is well worth noting at this point that FCA-issued certificates will, depending upon how implemented, be able to function as "unique national documents" and will thus implicate many of the personal liberties hysteria that proposals for such documents have generated in the past. Moreover, FCA-issued certificates will operate, and will be able to assist in storing, retrieving and indexing information in hidden and mysterious ways.

<sup>118</sup> Consider the following ATM credit card fraud (as recounted by the victim) when the lack of a *personal presence* requirement may have contributed to the success of the fraud:

Much more interesting, however, was how my PIN was obtained, allowing the perpetrators of the fraud to use a fake MasterCard in an ATM 4 times a day, 4 days in a row, \$500 each time . . .



**Ceremony (e.g., Oaths and Affirmations)**

**b. Direct/Internal Applicant Certification (Verified by FCA)<sup>119</sup>**

**c. Remote Applicant Certification (Verified by Notary)<sup>120</sup>**

**d. Humans vs. Organizations vs. Devices<sup>121</sup>**

---

Seems a written request for change-of-address was received by my Credit Union (backers of the MasterCard); this change was processed sometime on Wednesday, July 7th. The request included all sorts of identity-confirming information such as date of birth, social security number, and my mother's maiden name. The address was changed to a Brooklyn NY apartment (I live in a single-family house in Virginia).

IN THE SAME LETTER a request was made for a copy of the PIN for the MasterCard (not unusual for people to forget a PIN and request it again). The PIN, the most important secret piece of information for the card, was dutifully mailed off to the fraudulent address in Brooklyn.

Starting Monday, the 12th, the fraudulent cash advances were made from two different Brooklyn banks' ATMs.

R. Smith, *ATM Fraud/Databases/Ouch!*, Risks Forum List (July 19, 1993).

See Appendix C ("The Automation of the Notary Public"), *infra* (considering the requirements and benefits of personal presence for notarial acts).

An interesting parallel affecting liability exists between automated procedures to obtain certificates (without personal presence/interaction between the certificate applicant and the CA) and vending machines offering insurance policies. A key consideration is whether the insured is held to understand the policy: "when the potential insurance purchaser cannot consult with an agent to ascertain the parameters of the proposed policy the concept of an informed meeting of the minds is a myth unless the insurance company clearly and explicitly explains the policy in the literature. . . . In this situation more than any other, the company must be held accountable for misstatements and ambiguities in its literature." *Fritz v. Old Am. Ins. Co.*, 345 F. Supp. 514, 518 (S.D. Tex. 1973).

<sup>119</sup> See Section VIII.D.2.b. ("Notaries Internal to the CA"), *infra*.

<sup>120</sup> See Section VIII.D.2.a. ("Remote" FCA Notaries), *infra*. Such verification could also be completed by security officer or "LRA" (local registration authority).

<sup>121</sup> Whether the issuance of certificates should be limited to individuals, or extended to organizations and even to devices, requires consideration of the following factors:



## **B.2. Proof and Verification of CRD**

The designated person or persons who examine CRD and physically observe the certificate applicant's person (where personal presence are required) is indispensable to the integrity of the FCA and its certificates. The extent to which CRD evaluation can or should be delegated to non-FCA parties such as independent notaries public implicates significant management and legal decisions that affect liability exposure. Also, the consistency and extent of CRD evaluation (including of CRD examiners) requires consideration, particularly because there are few government-wide requirements for the issuance of federal employee identification credentials.<sup>122</sup>

### **a. Trustworthiness of Verifier<sup>123</sup>**

#### **Verifier Qualifications<sup>124</sup>**

---

- **Organizations/Users:** The critical issue is accountability. There is concern that improper use of a certificate issued to an organization will retard holding culpable persons responsible. In conventional practice, individuals sign documents in a representative capacity (based upon delegated powers, agency, etc.). In this respect, the argument goes, there is no reason that certificates (and corresponding key pairs) could not be issued to individuals as well as to roles/offices.

- **Devices:** Devices such as trusted time and date-stamping devices and multi-bank automated teller machines need to be identified in a verifiable manner. It is proposed that certificates be issued to devices so long as an individual or organization takes responsibility for their use/actions. The definition of *user* can be sufficiently broad to include device, *e.g.*, a *functional object* that engages in message handling and that is a potential source or destination of messages.

See Section IV.L. ("Use of Card Technologies"), *supra*.

<sup>122</sup> Notable exceptions include national security positions and, of course, passports. See Section XIII.F., *infra*.

<sup>123</sup> A "verifier," sometimes known as an *organizational notary* or *certificate management authority*, refers to a person who evaluates an applicant's credentials and application and issues certificates to appropriate users on behalf of a CA. Verifiers play a pivotal role in the FCA infrastructure and contribute to the trustworthiness of the FCA generally.

<sup>124</sup> Verifier qualifications are of utmost importance. Consider one distinguished commentator's assertion that "[t]he greatest threat to computer security is the unintentional act of an employee who is well meaning but negligent or poorly

## **Notaries Public<sup>125</sup>**

### **b. Investigation and Independent Confirmation**

#### **Verification of Conventionally Submitted (Paper) CRD**

#### **Verification of Electronically Submitted CRD<sup>126</sup>**

### **c. Authentication vs. Authorization of Certificate Verification<sup>127</sup>**

---

trained [and that t]he primary responsibility remains with management, and failure to discharge this responsibility faithfully could result in personal liability for officers and directors." R. Bigelow, *COMPUTER CONTRACTS -- NEGOTIATING, DRAFTING* § 15.02[1] (1992). *See* Violino, *Hackers*, *INFORMATION WEEK*, June 21, 1993, at 49, 54 (stating with regards to the hiring of hackers to provide security consulting and testing services that "hackers-for-hire have in fact been convicted of major crimes in the past").

<sup>125</sup> *See* Appendix C., *infra* ("The Automation of the Notary Public"). Notaries public are included herein because of their potential roles. Thus, a notary public might be employed by a CA for purposes of user-applicant identity verification, or an independent external notary public might acknowledge certificate applications prior to submission to a CA. Both of these roles are considered in Section VIII.D., *infra*.

When the binding between the user and his or her public key is verified by a notary public, the FCA loses a degree of control over the certification process, because the FCA cannot comparably represent the accuracy, authenticity, integrity, or reliability of information contained in the certificate except as a matter of faith. On the other hand, where a notary public (preferably one that is not employed by the CA) is involved, the FCA may possibly be able to transfer a degree of the liability risk concerning the integrity of the binding (to the notary).

<sup>126</sup> Verification of "electronically submitted CRD" may include both digitally signed and non-digitally signed CRD. "Non-digitally signed CRD" may include computer-based orthographically signed documents (*e.g.*, pen-based computer signatures that are recorded graphical representations of a hand-written signature rather than digital signatures). The trustworthiness of such non-digitally signed communications requires special consideration. This lack of trustworthiness is similarly a problem with the risk of edited fax images containing added or changed signatures. *See* Section IV. D. ("Availability"), *infra* (stating the assumption that third party service providers provide only availability and do not provide "services of authentication, integrity, confidentiality and non-repudiation").

<sup>127</sup> The issues and risks identified in this section concern authentication certificates rather than attribute (or authorization) or other certificates. *See* Section V.C.4., *infra*.



### **B.3. Naming**

The necessity of obtaining, registering and using naming information presents further potential bases for FCA liability.<sup>128</sup> If the Public Key Infrastructure is to be useful in a global context, as implied by the ISO Open Systems Interconnect architecture, then it is important that the naming process incorporate a unique identity, whereas users may desire, if not demand, the right to control their "name." External constraints imposed by domestic and international organizations and standards must also be accommodated, together with various requirements for privacy and ease of use. Satisfaction of each of these requirements and constraints is very difficult to achieve.

#### **a. Subject-Name Uniqueness; Distinguished Names<sup>129</sup>**

---

<sup>128</sup> In addition to the discussion in this Section V.B.3., naming issues are considered in Sections IV.G.; V.A.7.a., *supra* and Sections V.D.2.a.-b.; VII.A.5.; IX.C., *infra*.

<sup>129</sup> An Internet RFC provides a useful primer on name uniqueness issues:

Computer systems require a way to identify the people associated with them. These identifiers have been called "user names" or "account names." The identifiers are typically short, alphanumeric strings. In general identifiers must be unique.

The Uniqueness is usually achieved in one of three ways:

1) The identifiers are assigned in a unique manner without using information associated with the individual. Example identifiers are:

ax54tv  
cs00034

This method was often used by large timesharing systems. While it achieved the uniqueness property, there was no way of guessing the identifier without knowing it through other means.

2) The identifiers are assigned in a unique manner where the bulk of the identifier is algorithmically derived from the individual's name. Example identifiers are:

Craig.A.Finseth-1  
Finseth1  
caf-1  
fins0001

3) The identifiers are in general not assigned in a unique manner: the identifier is algorithmically derived from the individual's name and duplicates are handled in an ad-hoc manner. Example identifiers are:



---

Craig.Finseth  
caf

RFC: 1439, "The Uniqueness of Unique Identifiers" (March 1993).

While a public key certificate as specified in X.509 provides a mechanism for binding an entity's name to its public key, RFC 1422 allows this binding to be endowed with a more complex "semantic." For example, the FCA might establish a policy requiring an organization to issue certificates in a fashion that syntactically distinguishes among full-time employees, part-time employees, summer employees and contractors.

The PEM RFC "profile" of X.509 purports to restrict the Subject and Issuer fields to contain so-called *distinguished names* (DNs) [see definition in note 30, *supra*.], rather than simply *names*. This is in keeping with the text of X.509 § 7.2, which states, "A certification authority produces the certificate of a user by signing a collection of information, including the user's distinguished name and public key."

Accordingly, it is suggested that each CA entity take reasonable steps to verify that a DN uniquely identifies the subject user and applicable organizational entity (e.g., a specific division, department, etc.), and is not easily confused with other users and/or organizations. Each CA entity should also promptly notify its superior in the hierarchy of any changes to its certification hierarchy.

The time period during which a DN must be unique might include:

1. At the moment it is assigned, and for as long as the operator of the X.500 directory service chooses to provide the listing, e.g., for as long as the individual is a customer of the utility?
2. For the duration of the current X.509 certificate (if any)?
3. For as long as the individual is an employee or affiliate of the organization?
4. Until the expiration of the statute of limitations for (pick your crime)?
5. For 120 years after the birth of the individual in question?
6. For 50 years after the death of the individual in question?
7. Forever, or at least for the duration of the CA whose name forms part of that user's name under the name subordination rules?

E-Mail list posting by R. Jueneman, GTE Laboratories (July 27, 1993).

Because certificates are intended to provide a reliable binding between a public key and a user or certification authority, ensuring that DN's do not create confusion is important. While the structure of a DN technically ensures its uniqueness, it remains possible for human users to become justifiably confused due to similarities among DN's. While the application software employed by some

## b. Name Subordination<sup>130</sup>

organizations may provide sophisticated user-interfaces which alleviate potential naming confusion, the level of user interface sophistication may vary considerably both within the certifying organization and from one organization to another. Therefore, it is important to accommodate the lowest common denominator in user-interface technology. This policy will provide global benefits to the FCA community.

Also, the CA should ensure (to the extent feasible) that all public keys are unique. It is technically impossible for a CA to ensure that *all* public keys are unique in large systems, where multiple CAs may be signing new certificates simultaneously. Further, it may not necessarily be a risk to have duplicate public keys to the extent that holders of identical public keys share the same private key. See Memo from J. Lowry to M. Baum (July 30, 1993); see ANSI X9.30, *supra* note 5, § 4.2.1.5.

"If the key generation mechanism works properly, it is so unlikely that two different users will generate the same key pair, that we need not worry about it. However, when a holder registers a public key, the CA should check that the applicant knows the corresponding secret key. Otherwise [the applicant] may thwart the system by registering an already registered public key which of course will cause problems [a denial of service threat]." Memo From P. Landrock, *supra* note 13.

It has been suggested that "[a] CA may wish to certify only a portion of the DN of an individual. In particular, the CA might disclaim liability for correctness of an individual's personal name, since their signature is binding on their organizational sponsor in any event." Sudia & Ankney, *The Commercialization of Digital Signatures* § 4.2 (Paper presented to the Information Security Committee, EDI and Info. Technology Division, Section of Science and Technology, ABA (June, 1993). Or, the CA might hold itself out as affording a different level of service for each element of the name." *Id.* see also ANSI X9.30, *supra* note 5, § 4.2.2., at 12.

<sup>130</sup> Name subordination (*e.g.*, to the CA) is a technique for ensuring the unique nature of a subject name. However, an externally imposed subordination technique may not align with a directory naming policy already established by the subject or the subject's organization, which may already have governed the assignment of the party's distinguished name prior to certificate issuance by the CA. Subordination also ensures that a user cannot masquerade as a CA and issue false certificates signed by a legitimately certified key. Optionally, the FCA can use the semantics in a certificate (*e.g.*, the PEM RFC's X.509 profile) to indicate user, CA, PCA, etc.



- c. Accommodating User-Requested Naming<sup>131</sup>
- d. Authority to Use Organizational Affiliation(s)<sup>132</sup>
- e. Right or Privilege<sup>133</sup>
- f. Communities of Interest<sup>134</sup>
- g. Naming Registration Authorities<sup>135</sup>

---

<sup>131</sup> For obvious reasons, the FCA should not permit users to use trademarks or service marks belonging to others. Concerning a tangential name/user registration issue, *see* *Denny's Auto and Towing, Inc. v. Michigan Bell Telephone Co.*, 343 N.W.2d 550 (Mich. App. 1983) (awarding damages for lost profits and mental anguish arising out of phone company's negligent omission of plaintiff's telephone number and listing from directories).

<sup>132</sup> The extent of an applicant's *affiliation* with its organization is critical. Affiliation defines who is employed by, contracts with, or otherwise maintains a relationship with, the organization, thereby reasonably justifying the issuance of a certificate carrying a name associated with the organization. A standard of reasonableness is required of the CA in determining whether an applicant-user is properly affiliated. While it is anticipated that criteria for affiliation may vary among CAs, the user's relationship with its organization must be real and meaningful. Otherwise, global confidence in the certification process will suffer.

Also, consider the lack of confidence that may result from the policy prescribed in 12 C.F.R. § 205.6(a)(2) (financial institution not required to provide a means of identifying separate users in order to impose liability for unauthorized transfers when more than one access device is issued for an account). *See* BOARD OF GOVERNORS OF THE FED. RESERVE SYSTEM, OFFICIAL STAFF COMMENTARY ON REG. E 9 (as amended through Apr. 1987) (regarding electronic funds transfer).

One commentator suggests that liability for naming is of concern where it is: misleading, difficult/impossible to find (look up a name), or misrepresents an association. The CA may be required to determine that the name bears a reasonable relationship to the real world and also that the world perceives it as such. *See* Memo from Frank Sudia to Michael Baum (Aug. 28, 1993) (on file with Independent Monitoring).

<sup>133</sup> *See* Section IV.G., *supra*.

<sup>134</sup> *See* Section V.A.3.f., *supra*.

<sup>135</sup>

Standardization results in the requirement that objects be unambiguously identifiable on a global basis. These objects may be defined by organizations such as the International Organization for Standardization (ISO), the



---

International Electrotechnical Commission (IEC) . . . and commercial, and governmental organizations.

ISO/IEC and the International Telecommunications Union (ITU, formerly the CCITT) have jointly developed the Registration-hierarchical-name-tree (RH-name-tree). This is a tree whose nodes correspond to registered objects, and whose non-leaf nodes correspond to registration authorities. A registration authority is an entity such as an organization, a standard[s body], or an automated facility that assigns unambiguous names to objects. The root of the Registration-hierarchical-name-tree corresponds to CCITT X.660 Recommendation and ISO/IEC 9834-1 Standard.

R. Jueneman, *Naming, draft CA Name Registration Guidelines* (May 5, 1994) (copy on file with Independent Monitoring).

See C. Gillooly, *Novell Devises IPX Net Registry Service*, NETWORK WORLD, Apr. 19, 1993, at 13-14 (aiming to "aid in eliminating conflicts if the registered customers need to communicate with another company that has the same address. . . . Today, if a message is sent to a user that happens to have the same address as another user on another network, the network will react unpredictably. 'It may send the message to the wrong person, it may send half the message to one and half to the other or you may just get a bunch of error messages.'"). See North American Directory Forum (NADF), *SD-5: A Naming Scheme for C=US and C-CA* (1993); ISO 9834-1 (1993) (considering liability and contractual obligations associated with ISO and ANSI name registration); see also EDIRA, *Memorandum of Understanding for Operation of EDI Registration Authorities 3* (Final Draft, Nov. 30, 1993) (aiming to provide "a basis for global unambiguous identification of organizations involved in EDI. . . .") *Id.*

The ANSI *Request for Assignment of an Organization Name* includes the following disclaimer:

ANSI is a not-for-profit corporation. By reason thereof and in further consideration of the services rendered by ANSI hereunder, applicant agrees that (i) any claim it may have against ANSI arising out of this program shall be resolved exclusively through arbitration . . . and (ii) damages in such proceedings awarded against ANSU shall be strictly limited so as not to exceed the total amount of payments made by applicant to ANSI under this program. . . .

135A The COMMITTEE ON APPLICATIONS has recommended the use of DUNS numbers for trading partner registration. The relation among trading partner registration numbers and public key certificates demands further study. A DUNS number

## **h. Numbering<sup>135A</sup>**

### **B.4. Certificate Application Processing**

Certificate application processing must be well constructed both technically and procedurally so as to minimize claims of substandard procedures. The issues and potential exposure associated with certificate application processing involve timing, fairness, documentation, notification, retention and dispute resolution issues, together with various subsidiary issues. The application process should therefore be highly coordinated, prepared for contingency and exception processing and able to respond to any obligation to provide probative evidence in the event of a dispute or legitimate request for information.<sup>136</sup>

#### **a. Timeliness and Accuracy<sup>137</sup>**

---

is a widely used domestic and international commercial identification number for electronic commerce (54 U.S. industries and the United Nations use DUNS, for EDI); it is supported by a worldwide data collection program that focuses on maintaining an accurate data base of unique identification numbers (35 million numbers assigned worldwide); it is a validated numbering scheme (\$300 million spent annually to validate its accuracy as contrasted to TIN [Taxpayer Identification Number], which is not validated); it has worldwide support for numbering and positive identification of entities; its numbers are assigned to the lowest possible organizational business level (far lower than the TIN, which is a higher organizational control number); and it is issued at no cost to the Federal government or trading partner. Furthermore, the DUNS, number can be crosswalked against the other existing numbering schemes and can serve as a pointer to the data stored according to another numbering system.

Dun and Bradstreet has offered the Federal government a perpetual license to use the DUNS, number at no cost. . . .

COMMITTEE ON APPLICATIONS, *supra* note 23.

<sup>136</sup> See LINKING SECURITY, *supra* note 2, § II.a.2., at 33-37 (surveying evidentiary requirements).

<sup>137</sup> The FCA should process and approve or disapprove a certificate application within a set period of time (e.g., 30 days after its receipt). The FCA should be given final power to approve certificate applications, but should not unreasonably deny approval. See Section VI.F.3. ("Interference with Contractual Relations"), *infra* (concerning delaying the issuance of certificates).



## Processing and Issuance/Denial<sup>138</sup>

### Response to Applicant and Applicant's Organization<sup>139</sup>

#### b. Nondiscrimination and Fairness<sup>140</sup>

#### c. Retention of CRD and Other Information<sup>141</sup>

---

Failure of a user-applicant to provide accurate and complete information should be grounds for the FCA to deny or subsequently terminate the user's certificate. *Cf. supra* note 116.

<sup>138</sup> At the FCA's option, the FCA should have the right to confirm independently the accuracy of all CRD. Should the FCA disapprove the user application, the FCA should notify the user of the reason(s) for such disapproval within a specified period of time (*e.g.*, within 15 days of disapproval) and, where appropriate, permit the user-applicant to submit revised information.

<sup>139</sup> Upon approval of the certificate application (or upon approval of a CA's policy, where approval is required), the applicant should be notified explicitly. The user (or the CA, respectively) should carefully review the approval document for accuracy and completeness prior to commencing use. This may involve verifying the issuer's digital signature on the approval document. The user should notify the issuer promptly upon finding any error in such document.

<sup>140</sup> This may include giving equal or comparable treatment to both the FCA's own users *and* to interconnected non-FCA users. *Cf.* Section VIII.G.1. ("Regulation of United States Telecommunications"), *infra* (concerning relevant Open Network Architecture requirements). Because the FCA's infrastructure is not yet determined, the precise requirements concerning nondiscrimination and fairness cannot be assessed. However, fundamental principles of due process and fairness have been articulated and provide a useful foundation for FCA development.

<sup>141</sup> The retention of CRD and ancillary records may include internal processing documents, diverse memoranda, FCA-applicant correspondence, investigative materials and correspondence, certificates, CRLs, purchase orders, requisitions, checks, payment instructions, financial/accounting records and other forms of typical business information. *Cf.* Section V.D.7. ("CRL Retention") *infra*. The requirements for, and the propriety of, retaining records in paper vs. electronic form require careful review. *See generally* LINKING SECURITY, *supra* note 2.

FCA retention of CRD contributes to an audit trail, to the authentication of transactions, and to the resolution of disputes by assuring reliable proof of conduct. Retention requirements may be controlled by various laws and regulations, including the FRA and relevant case law. *See, e.g.*, Armstrong v.



#### d. Billing and Accounting<sup>142</sup>

Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993) (cited in note 95, *supra*).

To the extent that the records are classified as "Temporary" by an archivist under the FRA, or that the FRA is inapplicable, a default retention period (e.g., of seven years) should be considered for CRD, which is a period equal to, or greater than, many government records retention requirements (e.g., the Paperwork Reduction Act's three year default retention period and the IRS Rev. Proc. 91-59's seven year retention period; *see generally* Electronic Records Management, 36 C.F.R. Part 1234; 41 C.F.R. Part 201-45). Except for privacy-oriented or narrowly-focused legislation to the contrary, the FCA will presumably not be prevented from unilaterally expanding a CRD retention period. Also, *see* OMB Circular A-130, *supra* note 57. Indeed, there are strong advocates for the indefinite retention of certificates, CRLs and other information by the FCA. *See also* 36 C.F.R. Part 1234.28(f) (requiring "[d]uplicate copies of permanent or unscheduled records" [to] be maintained in storage areas separate from the location of the records that have been copied").

<sup>142</sup> If billing practices associated with certificate applications are automated, the formal use of financial EDI should be considered. *See generally* Model Electronic Payments Agreement and Commentary, *supra* note 2; NIST, *Electronic Data Interchange (EDI)* (FIPS PUB 161-1).

The reliance on automated procedures does have limitations. *See, e.g.,* Pompeii Estates, Inc. v. Consol. Edison Co., 397 N.Y.S.2d 577 (Civ. Ct. Queens Cty. 1977) (relying exclusively on computer readout to terminate electrical service does not demonstrate reasonable care); Price v. Ford Motor Credit Co., 530 S.W.2d 249 (Mo. App. 1975) (reliance on computer data as the basis for wrongful repossession); Ford Motor Credit v. Hitchcock, 158 S.E.2d 468 (Ga. App. 1967).

The liability associated with billing and accounting services was further considered in Shell Pipeline v. Coastal States Trading, 788 S.W.2d 837 (Tex. App. 1990), where a third party service provider's ("TPSP") responsibility for correction of errors was upheld, even when the TPSP's undertaking was "entirely gratuitous." The court reasoned as follows:

Shell claims that its computer system, which kept track of the trades as well as to whom the oil was to be delivered, was a mere gratuitous "bookkeeping record" for the benefit of its traders, and that Coastal's claim of contract fails for want of consideration ...

... Shell has assumed that responsibility of keeping its oil traders informed of any "mismatches" in names of parties to whom oil was consigned. Coastal relied upon this service, and when Shell failed to discover that the oil was to have been delivered to Basin, rather than to Basin Refining, Coastal lost its option to cancel the trade or to take

e. Audit Journal

f. Dispute Resolution Procedures<sup>143</sup>

C. CERTIFICATE GENERATION

C.1. Strength of Certificate

The technical evaluation of an FCA-created certificate's strength must consider the strength of the issuer's digital signature *sealing* the certificate as well as the strength and accuracy of credentials included in the certificate. From a liability perspective, however, the mere technical evaluation of a certificate's strength is not enough. Rather, it must be evaluated in terms of its anticipated and actual usage, the assertions (implied or express) made by the FCA as to its strength, and its use in the real world environment, including for the satisfaction of applicable business and legal requirements.

a. Algorithm, Key Size, and Other Parameters<sup>144</sup>

---

other steps to protect itself. This was all to Coastal's detriment. We hold that there was a legally enforceable contract between Shell and Coastal. We further hold that the failure of Shell's employees to discover and inform Coastal that there was a mismatch of nominations was a breach of a legally enforceable duty owed by Shell to Coastal.

*Id.* at 844. *Shell Pipeline* might become relevant to the FCA if the FCA were to provide accounting records or offer to "push" CRLs gratuitously. See Section V.D.6., *infra* ("CRL Updating and Promulgation").

<sup>143</sup> Here, "Dispute Resolution Procedures" concerns disputes among the FCA and certificate applicants, rather than among FCA users. Cf. Section V.A.2.g. (concerning resolution of *transactional* disputes among FCA users), *supra*; Section IX.D.4., *infra*.

<sup>144</sup> There is, of course, a voluminous literature, including technical standards, addressing algorithm, key size and other technical parameters of certificates. However, as noted above, the ultimate strength of certificates can only be assessed by considering the environment within which it is used. In this regard, a *catch-all* category ("d. Other/Environmental Factors") is included. Concerning key size, see E. Messmer, *Bellcore leads team effort to crack RSA encryption code*, NETWORK WORLD, May 2, 1994, at 14.

See NIST, *Memorandum For The Record of a Sept. 22, 1989 Meeting of the NIST/NSA TWG* (Columbia, MD) (noting in regards to the publication of a Federal Information Processing Standard (FIPS) on a Digital Signature Standard (DSS) [see NIST, *Approval of FIPS PUB 186, Digital Signature Standards*, 59 Fed. Reg. 26,208 (May 19, 1994)], that "NIST will assure that [the FIPS] will be carefully worded so as not to contain any real or implied liability to the government



**b. Meaning/Significance of Certificates<sup>145</sup>**

**c. Interworking<sup>146</sup>**

**d. Other/Environmental Factors**

**C.2. Certificate Validity Period**

The time period within which the FCA can or should issue a certificate, and within which a user can or should rely on a certificate, raises potential liabilities. For example, how far into the future an FCA should issue a certificate, and whether the law should distinguish between the reliance that a user places on a certificate prior to its validity period versus the reliance placed on that certificate immediately following its validity period, require clarification.

**a. Use Prior, During and Following Validity Period**

**b. Duration<sup>147</sup>**

---

concerning the strength of the algorithm"); *see also* M. Baum, *The Proposed Digital Signature Standard: Implications for Electronic Data Interchange*, 8 COMP. L. & SEC. REP. Issue 3 (Elsevier, Sept.-Oct. 1992) (surveying certain DSA and general digital signature liability issues, including some pertaining to algorithm, key size and other parameters).

There are also algorithm, management and control issues associated with implementations that utilize a single key pair for both authentication and privacy (*e.g.*, PEM).

<sup>145</sup> To the extent that no precise conventional analog to a public key certificate exists, there is an urgent need to be concise as to its meaning, assertions, and limitations. Various management and technical studies and reports, relevant standards development efforts, legal initiatives and pilots should contribute to a better understanding of certificate strength. *See* Section X., *infra* (concerning various recommendations intended to contribute to this understanding).

<sup>146</sup> *See* GULS (Generic Upper Layer Security), ISO/IEC Draft International Standard (DIS) 111586 (1993). Parts 1 through 4 thereof were recommended to become a DIS in June 1993.

<sup>147</sup> A certificate should be issued for a period not to exceed the validity period of its CA's certificate (unless perhaps the CA's certificate is recertified at a later date). A user who relies on a digitally signed message corresponding to an expired certificate or a certificate issued for a period longer than the validity period of its CA's certificate should be held responsible for any lack of validity or enforceability unless some other regime is expressly established. Although a preliminary observation, certificates are generally valid for a duration of two years or less. *Cf.* 22 U.S.C. § 51.33 (passports issued for 10 years unless restricted).



### **C.3. Certificate Issuance Propagation and Reissuance**

The issuance and propagation of certificates presents interesting and novel issues that require clarification. Without detailed rules and procedures, potential legal liabilities associated with certificates must be examined with a view towards conventional analogs.

#### **a. Push vs. Pull<sup>148</sup>**

#### **b. Extensions and Reissuance<sup>149</sup>**

##### **Following Erroneous Certificate Revocation**

##### **Following Correction/Resolution of Certificate Revocation**

---

<sup>148</sup> *Push* refers to procedures whereby the FCA delivers certificates and CRLs to specified users and entities. *Pull* refers to procedures where persons desiring certificates or certificate revocation status information either perform a directory *look-up* or submit a request to the FCA (or to an FCA designated directory/data base entity) in order to obtain certificates and certificate information.

Authentication and acknowledgment of both send and receive events will be important for both push and pull approaches.

<sup>149</sup> To minimize disruption of certificate issuance services, the FCA should develop a policy concerning extension or reissuance of certificates. One (preferable) policy option would prohibit certificate extensions. Another (discouraged) policy option would automatically extend certificates for a fixed period of time from its expiration date unless (i) some other period is specified, (ii) the user is in breach of FCA policies or agreements, or (iii) the user notifies the FCA prior (*e.g.*, upon 45 days notice) to the expiration of the current term, of its intention not to extend the certificate's validity period. Unless otherwise provided, the extension should be under the same terms and conditions as those of the initial period.

Regardless of whether certificates are extended or reissued, the FCA should specify in its policy statement whether the underlying credentials of a user will be reexamined prior to the extension or reissuance. *Cf.* 22 C.F.R. § 51.21(c) (U.S. passport renewal does not require personal presence). *See generally* Section VIII.F., *infra* (concerning passports).

## Upon User Request<sup>150</sup>

### c. Automation (Minimizing Human Involvement)<sup>151</sup>

---

<sup>150</sup> Procedures to accommodate changes of address and other user requests affecting certificate reissuance create fraud exposure. As a counter to pervasive real estate fraud, consider a recent legislative change to the notary laws of Los Angeles County which provides the record owner of real property with explicit notice from the registry that someone has attempted to defraud him or her by transferring the record owner's property. Cal. Gov't Code, Ch. 815, amending § 8206 (1992). Perhaps a comparable explicit notification requirement would bolster the trustworthiness of certificates when reissuance is based upon user request.

<sup>151</sup> Automation of the certificate and CRL generation process raises legal issues that parallel certain expert systems and artificial intelligence legal issues. *See Cole, Tort Liability for Artificial Intelligence and Expert Systems*, 10 COMPUTER L.J. 127 (1990). The existence (or lack) of "override" mechanisms to reach a live human in automated "voice mail" systems presents similar problems. Query whether the lack of such mechanisms might present liability exposure to persons attempting to make contact in an emergency when there is an obligation to respond. Assuring the availability of appropriate controls that permit human involvement in exigent circumstances is important. Note that the term "expert systems" is "rechristened rule-based systems." *See Playing By the Rules*, INFORMATION WEEK, May 2, 1994, at 40.



#### C.4. Attribute and Other Certificates<sup>152</sup>

In conventional paper-based practice, authority for the acts of an entity's agents is often *apparent* or *implied*.<sup>153</sup> In computer-based practices, there is considerable interest in, and pressure for, creating infrastructures that provide more certainty than is available in many conventional environments (*e.g.*, by providing mechanisms to communicate *express* authority). This is so either because of fear that computer-based practices are inherently of greater risk than are conventional practices, or because of the desire to explore the new opportunities that computer-based environments offer. Consequently, a spiraling number of proposals are urging the development and standardization of novel certificate types with functions that vary from, and expand upon, those of a "standard" authentication certificate.

While implementation of such proposals can offer greater transactional certainty, there are many questions deserving of consideration that highlight the complexity and extent of attribute certificate issues. For example, what liability impact might the use of authorization certificates have on systems and applications that implement them as a matter of

---

<sup>152</sup> "The attributes associated with an entity are carried in a separate structure which is signed by an Attribute Authority (AA) [A CA may also be an Attribute Authority]. This structure is the attribute certificate (**AttributeCertificate**). This is a separate structure from the public key certificate (in order to maintain conformance with existing international standards). An entity may have multiple attribute certificates associated with each of its public key certificates." ANSI X9.30, *supra* note 5, § 5.6, at 35; *see* ANSI X9.45, *supra* note 71.

It is the author's understanding that, as currently proposed, the FCA is anticipated to accommodate attribute certificates. One argument against the adoption of attribute certificates reflects certain (paper-based) practices whereby authority is frequently not expressly communicated. Should there arise a need for attribute certificates and the FCA does not issue them, then the obvious question as to their source arises. If an entity other than the FCA issues attribute certificates, the subject of each certificate may require a separate key pair (unless perhaps that key is linked back to a user's authentication certificate and its key). The FCA should architect an efficient and effective way to accommodate such a "quasi-parallel" structure.

There may also be instances when delegation is intended to be effective only for a brief period of time, perhaps even minutes or seconds or for a single nearly instantaneous transaction. *See* Sudia & Ankney, *supra* note 129.

<sup>153</sup> *See* Section VIII.C., *infra* (addressing agency issues).



prudent practice? Should the law impute authority running from authentication certificates irrespective of the use of attribute certificates? To what extent should the existence of authorization or other attribute certificates be assumed and relied upon by message recipients when only an authentication certificate is received and such certificate's structure does not indicate the existence or availability of an attribute certificate? Should legal presumptions favor a certificate-based bifurcation of authentication and authority? The failure to resolve these issues will engender both confusion and the likelihood of mistaken assessments of the authority of FCA-supported digital signatures.

**a. Delegation Certificates**

**b. Virtual Certificates<sup>154</sup>**

**c. Sponsor Certificates<sup>155</sup>**

**d. Other Certificates**

**Persona Certificates<sup>156</sup>**

---

<sup>154</sup> A *virtual certificate* is defined as a certificate that is issued internally for the exclusive internal use of an organization, following the verification of an external entity's certification chain. The virtual certificate includes the external entity's public key, and is maintained on the organization's internal directory for the purpose of providing an expedited mechanism for verification of external (e.g., vendors') certificates. Telephone Interview with L. Shomo, National Aeronautics and Space Administration (Washington, D.C., July 21, 1993). The certification path/validity must be checked against CRLs periodically, or perhaps upon receipt.

An alternative definition for a virtual certificate is a data structure created for internal use within an organization that corresponds to a verified certificate and that is subsequently used by the organization to expedite verification of corresponding digitally signed messages. This can also be defined as a "chain-certificate," in that it substitutes for a chain of certificates which the user need not retrieve and process.

<sup>155</sup> A *sponsor certificate* is "intended to close the gap between user certificates and attribute certificates. Basically, we can impose the off-line authorization control model through the attribute certificates, but the sponsor certificate goes one step further. An entity named higher up in the user's relative distinguished name can say 'hear ye, we will be legally bound by this user's signature only if you present a set of attribute certificates meeting the following criteria:' [etc]. This would fulfill [a requirement for] full, explicit, machine-only, verifier-driven enforcement of the restrictions." E-mail from Frank Sudia to Michael Baum (June 19, 1993).

<sup>156</sup> *Persona certificates* (issued by a CA without assertion as to the subject's identity) and *self-signed certificates* (issued by the signer) have been proposed for certain public key systems and have already appeared in others. This paper takes

## Self-Signed Certificates<sup>157</sup>

### e. Different Keys/CAs for Authentication & Attribute Certificates

### f. Certified Time Stamps<sup>158</sup>

---

the position that neither of these certificates will be used because they fail to satisfy FCA needs. "I question whether the citizen of any free country has a general right to anonymity, that is, the freedom to act without being accountable to society. . . . To my mind, anonymity is a fantasy." P. Redfern, *Precise Identification through a Multi-purpose Personal Number Protects Privacy*, 1 Int'l J. of L. & Info. Tech. 305, 308 (Winter 1993).

<sup>157</sup> The propriety of self-signed certificates has been a point of contention, and viewpoints within the public key community are quite diverse, as indicated by the following communication.

[Question:] >So, is a self-signed certificate a security risk? No, but trusting one is. Your conclusion assumes that I have some contact with the person in question besides via e-mail.

If I "met" the person through e-mail (or postings) and have communicated only that way and if all of those messages had been signed by the same key – then if I get a self-signed certificate signed by the same key, I have received \*proof\* that this certificate is really for that person. It is totally trustable.

In this case, "that person" means literally "the person who knows the private key to match this public one" – it says nothing about the person's name or occupation or employer or even about how many flesh-and-blood humans constitute that "person." (E.g., the boss's secretary signs his letters to some people; even writes them to some.)

For many of my e-mail contacts, this is a fair description. I have never met the person, I probably never will and I really don't care who the person's employer is, what the person does for a living or what the person's name is on his/her birth certificate. All I care about is that this is the same person I've been conversing with all this time.

E-mail posting of Hoyt Kesterson, Bull Worldwide Info. Systems (June 11, 1993).

<sup>158</sup> See LINKING SECURITY, *supra* note 2, § II.e., at 44-45 (surveying time stamping cases and legal issues). See also *Timpinaro v. SEC*, 2 F.3d 453 (App. D.C. 1993) (upholding the "15-second rule" for automated trading). One advanced form of digital time stamping is described in B. Cipra, *Electronic Time-Stamping: The Notary Public Goes Digital*, SCIENCE, Jul. 9, 1993, at 162-63.



## **g. Liability for Information Content<sup>159</sup>**

### **C.5. Controls for Certificate Generation**

Controls for certificate generation must be commensurate with its risks. The potentially catastrophic level of harm that could be inflicted by FCA malfunction suggests the conclusion that responsible controls will likely be viewed by the legal system as requiring a comparatively high standard of care (subject, of course, to applications, systemic and transactional values and other recognized criteria).<sup>160</sup>

#### **a. Prevention of Forgery and Unauthorized Use**

##### **Hardware vs. Software Certificate Generation<sup>161</sup>**

##### **Certificate Issuance Hardware<sup>162</sup>**

---

<sup>159</sup> An attribute certificate can contain multiple elements of authority. When each of such elements is delegated or approved by different people within the issuing organization, the absence of a [digital] signature from each of the authorizers may weaken the intended accountability. If an entity subordinate to the authentication certificate issues an attribute certificate, the nature and extent of requisite compliance with the rules of the superior entity must be determined.

<sup>160</sup> Cf. Section VI., *infra* (concerning ultra-hazardous activities and strict liability).

<sup>161</sup> There has been considerable debate and political capital expended among federal agencies in seeking to develop a policy to resolve whether certificate generation (as well as key generation/storage) should or must be undertaken within a hardware (trusted) or a software environment. Many of the issues involve cost and parallel those concerning the use of card technologies. See LINKING SECURITY, *supra* note 2, § III.b., tbl. 4, at 52 (surveying costs in implementing cryptographic methods).

<sup>162</sup> Hardware is available (for example, RSA markets BBN's Certificate Issuance System (CIS)) to provide stringent controls on the type and scope of certificates which a CA may sign. It has the capability to (i) communicate directly or indirectly with the host processor that submits certificate requests, (ii) utilize a private key to sign a validated certificate request, and (iii) accept and/or store cryptographic keys in a trusted manner and employ suitable cryptography to verify that a private component corresponding to a CA remains undisclosed beyond the CIS. CIS technology places constraints on issuer names, subject names, validity periods and serial numbers of certificates. It also specifies the public component for certificate validation. See RSA Data Security, Inc., *Certificate Issuing System*<sup>TM</sup> (product brochure) (1993).



**b. Audit Trail<sup>163</sup>**

**c. Retention of Current or Expired Certificates<sup>164</sup>**

**d. Confidentiality of Certificates<sup>165</sup>**

**D. CERTIFICATE REVOCATION**

**D.1. Authority to Request and Revoke Certificates**

A certificate-based public key implementation generally requires the use of Certificate Revocation Lists ("CRLs") to provide timely information about certificates revoked for specified reasons.<sup>166</sup> There are as of yet no

---

<sup>163</sup> Because the FCA may undertake diverse (and novel) responsibilities, many of which have yet to be articulated, there is a compelling rationale for implementing a particularly robust audit trail that goes beyond mere legislative and regulatory compliance. The inspector general's services of each agency performing FCA-related functions should review, or at least intimately participate in the development of, that agency's audit trail requirements. *See* ANSI X9.30, *supra* note 5, pt. 3, app. D (concerning audit journal requirements).

<sup>164</sup> Various approaches to certificate retention are possible, and include (i) retention of current certificates, (ii) retention of all current certificates plus the retention of expired certificates for a specified period, (iii) retention of current and expired certificates indefinitely or until the tolling of the outward limits of all required retention periods, or (iv) retention of CRLs that are time stamped in a trusted fashion and which represent that prior CRLs did not contain certain certificate serial numbers. The selection of an approach must be made in conjunction with a comprehensive retention program and strategy. Retention issues are also considered elsewhere in this Report, including within Section V.B.4., *supra*, and Section V.D.7., *infra*.

<sup>165</sup> There are instances when certificate holders do not desire disclosure of their certificates to anyone other than to a predefined and limited community. This is similar to individuals desiring to keep their phone numbers unlisted, or corporations desiring not to disclose their employee list for competitive (head hunter avoidance) or operational (restricting customers' contact to designated employees) reasons.

<sup>166</sup> A CRL is a list containing statements that the binding asserted by a CA between names and public keys for certificates on the issued CRL are dissolved. A CRL has also been viewed as a notification that the private keys corresponding to certificates placed on a CRL are no longer valid.

recognized national or global conventions for CRL procedures and expectations, although such conventions are being developed within ANSI X9.F1 and elsewhere. For example, the period of time between regularly scheduled CRL intervals, and the extent to which a user may rely on certificate validity during that time, remain unresolved. Another class of CRL issues concerns the rights of agents, employers, government officials, fiduciaries and other persons in positions of trust to request the revocation of certificates. These issues require further study.

**a. Delay/Failure to Submit a CRL Request:**

**To Superior CAs**

**To Cross-Certified CAs**

**b. Revocation of Employee Certificate upon Employer Request<sup>167</sup>**

**c. Revocation of Certificate upon Request of Subject's Agent<sup>168</sup>**

**d. Law Enforcement<sup>169</sup>**

**D.2. Basis for Issuing CRL**

The basis for issuing a CRL generally falls into one of three categories: key change or compromise; change of CA policy or cessation of CA operations; and user request.<sup>170</sup> The permissible boundaries for each category have not

---

<sup>167</sup> The permissibility of certificate revocation by an employer may depend upon whether or not the affiliation with the employer is stated in the certificate.

<sup>168</sup> See generally Section VIII.C. ("Escrow and Other Legal Agents"), *infra*.

<sup>169</sup> Procedures should be developed to control law enforcement requests or court orders for the revocation of certificates. Such procedures are warranted given the documented instances of illegal law enforcement compulsion of computer-based bulletin board operators to exclude alleged hackers without due process of law. When a court order is presented to a CA, procedures should ensure, *e.g.*, that a CA relied in good faith on a facially valid court order. See 18 U.S.C. § 2520(d); *cf.* Jackson v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex 1993). See generally Podesta & Sher, *Protecting Electronic Messaging: A Guide to The Electronic Communications Privacy Act of 1986* (1989) (providing sample TPSP procedures and guidelines intended to satisfy the Electronic Communications Privacy Act of 1986 -- notwithstanding differences in subject matter, Podesta provides useful background material to consider in contemplating the development of FCA procedures); Section VI.G. ("Criminal Liability"), *infra*.

<sup>170</sup> Other bases for issuing a CRL might include name expiration or change or non-payment by a user of an applicable user fee.



been comprehensively articulated. Inappropriate issuance of a CRL that revokes a CA's certificate can result not only in the cost of reissuing certificates, but also in the potential for tremendous consequential damages resulting from the interruption of business operations.<sup>171</sup>

**a. By the FCA**

**Key Compromise<sup>172</sup>**

---

<sup>171</sup> Cf. Section VII.A.1., *infra* (hypothetical case where an improper CRL issuance results in a crisis of constitutional dimensions).

<sup>172</sup> See Section V.A.2.h., *supra* (discouraging FCA key generation and management roles). However, if the FCA does undertake such roles, it should impose stringent safeguards against mistakenly or wrongfully disclosing users' private keys, including to a user's own organization. If a user's private key is compromised by the FCA, or if the FCA has reason to believe that there may have been a compromise, the FCA should use stringent efforts to notify all affected parties promptly of the relevant facts by, *e.g.*,

- a. sending a digitally signed message to the user (and, where applicable, the entities with which the user is affiliated);
- b. telephoning the user, *et al.*;
- c. notifying the user via express courier; and
- d. distributing a corresponding CRL in conformity with the applicable PCA policy statement.

Following a private key compromise by the FCA, the FCA, at the user's request, should (i) quickly (*e.g.*, within one business day) generate and communicate a new certificate for the user containing a new public key, (ii) promptly sign and reissue all current certificates previously issued under the old, compromised private key; (iii) bear (with respect to the user) all reasonable direct costs for re-registering the user with the FCA or with another CA, and (iv) notify the user of the cause of the compromise, if known, and any remedial actions taken to mitigate the possibility of future compromise, provided such disclosure by the FCA to the user does not in itself threaten or potentially threaten FCA infrastructure security.

Consider the following:

If a CA does change its key pair, then it would have to re-sign subordinate certificates, but there is no need for CAs or users of these re-signed certificates to change their key pairs, so the process does not propagate for more than one tier. Also, there is not a requirement that the subordinate certificates be immediately hot-listed. It depends on why the CA changed its key pair. If there was no compromise, it is likely that the reissuance process would be performed gracefully, with new certificates issued well in advance of when they would be required (the VALIDITY field in a certificate makes it easy to do that), to smooth the transition.



**Perceived or Threatened Compromise<sup>173</sup>**  
**Certificate Information Change**  
**"Critical" vs. "Noncritical" Information**  
**Naming and Affiliation**  
**Cessation of Operations**  
**Changes in Policy; Certificate Hold Notice<sup>174</sup>**  
**b. By the User**  
**Key Compromise<sup>175</sup>**  
**Perceived or Threatened Compromise**  
**Certificate Information Change**

---

S. Kent, E-mail List (June 15, 1993).

<sup>173</sup> See MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, *supra* note 2, § 10.2 ("Suspension of Operations") & Comments B.2.-B.3.

<sup>174</sup> Change in Policy: The "majority" position of public key developers suggests that any change in a PCA's policy, whether "critical" or "noncritical," requires that the CAs operating under that PCA be placed on a CRL because only (and to the extent that) material information should be included in a PCA policy statement and because PCA policies are not anticipated to change frequently.

Certificate Hold Notice: This is "a different type of CRL which doesn't actually revoke the certificate, but merely 'flags' it as suspect, with a reason code of 'unauthenticated revocation request,' while optionally giving any would-be verifiers some instructions on what to do until the matter is cleared up." It is anticipated to be used "where a CA must make a revoke/no-revoke decision without adequate information." "If the CA revokes wrongly, it could require a subordinate CA to invest millions of dollars to redistribute a public key that might have been embedded in millions of hardware modules, and recertify all their users . . . [and incur] potential damages for lost profits and injury to credit and reputation." F. Sudia, *Unauthenticated Certificate Revocation Requests: Certificate Hold Notices, Certificate Hold Released and Exception Handling Instructions*, ANSI X9.F1 (April 6, 1994).

<sup>175</sup> See ANSI X9.30, *supra* note 5, § 4.2.2. (proposing user responsibilities regarding key integrity). Note should be taken of the possibility of an entity intentionally compromising its private key in an attempt to avoid its commitments -- perhaps as the "crypto-equivalent" to declaring bankruptcy, although the likelihood of this affecting a well-implemented system is unsubstantiated.

**"Critical" vs. "Noncritical" Information**  
**Naming and Affiliation**  
**Cessation of Operations**

**D.3. Proof and Verification of CRL Requests**

A fraudulent or erroneous submission of a CRL request could potentially be devastating if, for example, the certificate's revocation were to affect public services such as fire alarms, water pumps, dams, air traffic control systems or telecommunications switches. The revocation of a certificate is irreversible. Accordingly, proof and verification of CRL requests should be carefully scrutinized.

**a. Investigation of Validity and Authenticity<sup>176</sup>**

**b. Establishment and Adherence to CRL Request Rules**

**D.4. CRL Keys**

It is generally contemplated that CRLs will be digitally signed using the private key that issued the corresponding certificate. However, other approaches offer other benefits and risks. For example, ANSI X9.30 requires that different keys be used for certificate and CRL issuance.

**a. Use of Different Keys for CRL and Certificate Issuance**

**D.5. CRL Validity Period**

The CRL validity period incorporates the interval between regularly scheduled CRL issuance. The length of a CRL's validity period should be commensurate with perceived risks and should also be *event driven*. In this respect, each PCA might establish a specific validity period. A CA should also, of course, generally have the option of varying (further limiting) a validity period on the basis of established criteria. The CRL validity period cannot be evaluated without considering the many controls and procedures that, taken as a whole, affect the trustworthiness of the FCA environment.

**a. Nature of Activity**

**b. Specificity<sup>177</sup>**

---

<sup>176</sup> Human, rather than exclusively machine interaction, should be required in the review of CRL requests. *See* Thompson v. San Antonio Retail Merchants Ass'n, 682 F.2d 509 (5th Cir. 1982) (imposing liability as a result of automatic information capture feature which did not evaluate the offered information for accuracy).

<sup>177</sup> X.509 CRLs do not indicate their next date of issue, whereas PEM CRLs provide information as to both issue date and next date of issue. The FCA

### c. Non-Repudiation vs. Origin Authentication<sup>178</sup>

---

infrastructure should ensure that the next date of issue is effectively communicated in a manner that is consistent with the technical structure and content of its certificates.

<sup>178</sup> This distinction concerns the legal implications of a CRL and a user's willingness (perhaps based on business risk) to accept CRLs for message origin authentication versus requiring non-repudiation, the latter properly requiring the "next CRL" unless alternative rules (including, *e.g.*, presumptions) are established:

For non-repudiation purposes, the requirement is really to have the CRLs issued AFTER the message was signed, so that they cover the interval during which the message was signed. Having the CRLs issued before the message was signed still leaves open a window of vulnerability for repudiation. I think this illustrates a difference between the more casual processing of a signature for message origin authentication vs. non-repudiation. For authentication, most users are probably willing to live with validation against the "current" CRL, whereas for non-repudiation, it is the next CRL that is required. Of course, people may choose to initiate delivery of goods based on a current CRL check, and live with the consequences, especially for small-value transactions.

S. Kent, E-mail List (June 16, 1993).

This may require that each user have a "current" CRL available; there might also be an online *hot list*. See Section IV.D., *supra* (assumptions include a requirement of non-repudiation). "Of course even the 'next' CRL is not proof that compromise or misuse *did not* occur. Rather, it only demonstrates that it had not yet been detected. Features such as co-signatures and confirm-to attributes can greatly mitigate these risks." Memorandum from F. Sudia (Nov. 12, 1993, on file with Independent Monitoring).



#### **D.6. CRL Updating and Promulgation**

The various methods for updating and promulgating CRLs offer opportunities and risks. One major decision concerns whether, as a default/baseline, to *push* or *pull* CRLs. To evaluate this issue properly, the costs of a push strategy (including telecommunications costs), legal requirements,<sup>179</sup> risks and, of course, the overall level of assurances which the FCA desires must be meticulously considered.

a. Push<sup>180</sup>

b. Pull<sup>181</sup>

---

<sup>179</sup> Legal implications include the distinction between *actual* and *constructive* notice. CRL policies must address the need for "adequate" or "reasonable" notice. There may be differences in push versus pull as to sufficiency of notice. This must be evaluated, in part, in the context of the status of the people using the FCA (e.g., considering the differences between consumers and nonconsumers, and between internal government users, external contractors, the public-at-large, etc.).

<sup>180</sup> "Push" refers to the FCA being responsible for promulgating CRLs -- "pushing the CRL to the user community." A push strategy places a greater burden on the FCA, unless, of course, special presumptions are established favoring the FCA. It is best to develop a flexible approach, since it is currently not clear what will ultimately be required. Cf. *Revocation Certificates* (generally contemplated to be "pulled" from a directory), Section V.A.2.b., *supra*.

Concerning PEM, it has been suggested that:

1. CAs push CRLs to children [persons certified under that CA] periodically.
2. Others can subscribe to CRLs and receive them at the time of push (delayed pull).
3. Anyone can do an immediate pull. . . .

S. Kent, E-mail List (June 15, 1993).

A CRL policy should consider requiring the CA to send all CRLs issued to a widely accessible network information center within a short period (e.g., two business days) following the FCA's receipt of a CRL request based on key compromise or "critical information" change. *See id.*

<sup>181</sup> "Pull" refers to users being responsible for downloading or otherwise obtaining CRLs from the FCA. A pull strategy may create greater or different legal risk to the FCA (particularly where the law requires actual and nonrepudiable notice). In an interesting parallel, consumer laws generally require an insurance company to send a notice via certified mail, return receipt requested before terminating insurance for nonpayment (a "push").

c. Scheduled<sup>182</sup>

d. Unscheduled<sup>183</sup>

---

<sup>182</sup> CRL requirements require evaluation for differing applications. Therefore, even if there is a CRL pushed every x hours or days, there may be a need to do an interim pull due to the higher risks associated with a particular document. The optimal interval for scheduled CRL issuance will vary.

A policy could be established requiring non-CA user organizations to notify their CA of the serial numbers of its user certificates that are to be included in a new CRL prior (*e.g.*, one business day) to the next regularly scheduled date for CRL issuance, even if there have been no changes in the CRL entries. Each CA could be required to issue a regularly scheduled CRL request no more frequently (*e.g.*, weekly) and no less frequently (*e.g.*, monthly) than the regularly scheduled interval for CRL issuance. If the organization fails to direct a CRL request to the FCA as required, and after (i) notice by the FCA to the organization of its failure to send the CRL request, and (ii) the continued failure of the organization to issue the CRL request promptly, the FCA could then have the authority to issue a CRL revoking the organization's certificate.

When the CA generates certificates, it should issue a new CRL request (*e.g.*, one business day) prior to the next regularly scheduled date for CRL issuance by the FCA, even if there have been no changes in the CRL entries. The organization should issue a regularly scheduled CRL no more frequently than (*e.g.*, three days; or weekly) and no less frequently than, *e.g.*, monthly. If the organization fails to issue a CRL as required, then the FCA may thereafter issue a new CRL revoking the organization's certificate (i) after notice by the FCA to the organization of its failure to issue a timely CRL, and (ii) the continued failure of the organization to promptly issue the new CRL.

PEM RFC 1422 addresses these concerns in the following way:

[P]redicting the time interval over which the next CRLs can be acquired is completely deterministic and addressed. Each PEM CRL carries a **NextUpdate** field that specifies the next scheduled issuance time and date for that CRL. Examination of this field tells a user (UA) when to request the next scheduled CRL for each PCA and CA. Obviously the CA/PCA in the path with the most distant (in time) **NextUpdate** time is the gating factor.

S. Kent, E-mail List (June 16, 1993).

<sup>183</sup> Unscheduled CRLs should be issued in the event of actual or perceived security compromises, change(s) in critical user information, or upon discovering a material mistake in a current CRL. However, the FCA generally need not issue a



**e. Garbled, Lost, Delayed and Misrouted CRLs & CRL Requests<sup>184</sup>**

**f. Reason Codes for CRL Issuance<sup>185</sup>**

**g. Availability of Global CRL Data Base to Users<sup>186</sup>**

---

request for an unscheduled CRL if the organization learns of the compromise, change or mistake within a short predefined period (*e.g.*, two business days) preceding the next regularly scheduled CRL. The entire CRL must be signed by the FCA.

<sup>184</sup> The apportionment of responsibility and liability for garbled, lost, delayed or misrouted CRLs should be developed with reference to the extensive work completed on this subject within the banking and EDI communities. *See, e.g.*, U.C.C. Art. 4A; *see also* MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, *supra* note 2, § 6.3; *cf.*, U.C.C. § 9-402(8) ("A financing statement complying with the requirements of this section is effective even though it contains minor errors which are not seriously misleading.").

<sup>185</sup> The issuance of a CRL that revokes a certificate and includes a *reason code* known by the CA to be false could be actionable as libel if, for example, a particular reason code erroneously indicates a criminal conviction. *Cf.* Section VIII.F. *infra* (State Department can refuse or revoke a passport upon conviction of a felony). Even when the false reason code is the result of simple error, the consequences could be considerable.

<sup>186</sup> Issues include the use of, and desirability of access to, CRLs from a PCA that a given user's PCA is not willing to certify. R. Jueneman, E-mail List (June 1993). Every PEM PCA is required (per RFC 1422 § 3.4.2.5) to provide an interface to a global CRL database, and every user is expected to know the E-mail address of his PCA. Evaluation of the global CRL data base is beyond the scope of this Report and requires further study.



### **D.7. CRL Retention**

A CRL retention strategy must consider the potential for action by parties on whose behalf the FCA is obligated to reproduce archival CRLs. Third party beneficiaries must also be considered. Moreover, the accelerating reduction in data storage costs, and the trend in EDI industry practices to sequentially capture all (or most) communications, provide ample evidence in support of a comparatively inclusive retention policy. The retention of CRLs and supporting transactional and system-related data should be carefully evaluated with respect to private and public retention requirements.

#### **a. Archival Methods**

**Retention Period**<sup>187</sup>

**Full vs. Partial Archives**

**Archives of Non-FCA Hierarchy CRLs**

**Retention Media**<sup>188</sup>

---

<sup>187</sup> A retention policy that expressly details requirements and procedures for all information originating or received by the FCA should be developed, including certificate applications, internal administrative memoranda, certificates, audit logs, periodic review of audit logs by auditors, CRL requests and CRLs.

Also, consideration should be given to the Federal Records Act as construed by *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993) *supra* note 95 (determining, in part, that E-mail constitutes a "record" under the FRA and may therefore require permanent retention). In the PEM model, there is no requirement that PCAs or CAs archive CRLs forever. Rather, the model adopted in PEM places the burden on the user to retain the necessary CRLs if non-repudiation is a concern. However, a PCA might establish long-term CRL archives if it believed that its subscribers would view this as a value-added feature. And yet, we may need to archive CRLs for 50 years to prove 50 year old digital signatures.

<sup>188</sup> See National Archives and Records Administration, Electronic Records Management Regulations, 36 C.F.R. § 1234.28 (concerning selection and maintenance of electronic record storage media). The decay of media and lack of compatible readers is a serious problem with valuable CPU data from the 1960s and 1970s. Any such policy, therefore, must contemplate forward copying of archives to the latest media.

**b. Time and Date Stamping<sup>189</sup>**

**c. Revision of Retention Policies<sup>190</sup>**

---

<sup>189</sup> The potential use of trusted time stamping of certificates and CRLs to reduce the scope of retained information (the complete certificate/CRL chain) deserves further study. See LINKING SECURITY *supra* note 2, § II.e., at 44-45 (discussing time stamping).

<sup>190</sup> Whether an FCA could update its policy, *e.g.*, by adding "non-conflicting" clauses intended not to compromise the security of existing certificates, without revoking all certificates previously issued under that policy deserves consideration. This would appear possible if the original policy put users on notice and thus contractually bound them to accept timely policy modifications. The FCA could indicate changes by a reason code in the CRL.

It is quite common for entities (networks, bank card issuers, and small businesses) to modify or update agreements. This will be particularly important in the case of public key cryptography, where not all the risks are understood because the activity is still relatively new. In this regard, CAs that seek to improve their policies (so long as the improvements do not materially change its user's obligations) should not be penalized.

## VI. LEGAL CONSIDERATIONS

### A. PURPOSE AND POLICIES OF LIABILITY

Rules of liability<sup>191</sup> are established to promote diverse societal policies. Such policies address the assignment of responsibility, including the legal right of compensation for harm, in furtherance of various goals such as behavior modification or deterrence,<sup>192</sup> economic engineering<sup>193</sup> and fairness.

The development of an appropriate FCA liability scheme will require the balancing of competing private and public interests and the handling of economic and social policy issues. A tentative goal might be to provide a liability scheme that will overburden neither providers nor users of FCA services with responsibility for risk, while providing a rational, intuitive and predictable compensation scheme for those injuries that do occur.

That some form of FCA legal responsibility/liability is desirable is beyond question. One information security expert has indicated that he would be "extremely reluctant" to absolve a certification authority from liability in the event a certificate were compromised because this would seriously diminish its incentive to perform responsibly. Without potential liability, there is no economic incentive to do a good job.<sup>194</sup> An Internet user's statement on CA

---

<sup>191</sup> "Liability is a broad legal term which is usually held to include every kind of legal obligation, responsibility or duty, certainly all that are measured by money obligation." *Mayfield v. First Nat'l Bank*, 137 F.2d 1013, 1019 (6th Cir. 1943). The term "liability" can also be used to express vulnerability to criminal law sanctions, to sanctions imposed by regulatory agencies, to loss of privileges granted or denied through an agency and/or an injunction in civil proceedings.

<sup>192</sup> The most noteworthy exponent of this view is, of course, Jeremy Bentham. *See, e.g., J. BENTHAM, THE PRINCIPLES OF MORALS AND LEGISLATION* (1948).

<sup>193</sup> A singularly convincing exploration of this theme in the context of the common law is M. HORWITZ, *THE TRANSFORMATION OF AMERICAN LAW, 1790-1860* (1977).

<sup>194</sup> *See* Telephone Interview with Sandy Epstein, President, Racal-Guardata, Inc. (May 27, 1993). Mr. Epstein also noted that to the extent that certificate-based public key implementations are viewed as containing inherent technical flaws, there can be no comfortable answer, adding that a CA without liability "intrinsically bothers me." *Id.*



liability reflected concerns and expectations of the many users: "Why in the world would anybody use a CA which accepted no liability for its actions? If I am going to pay money to a CA, I expect something in return!" Again, "[A]re we mortals, who invented the computers, enslaved to their correctness? Or do we still have the intellectual right to question their propriety, authenticity, reliability, and the possibility of malfunction?"<sup>195</sup>

This Report considers FCA liability largely in terms of potential exposure under current law. It also considers, where appropriate and instructive, the benefits to be derived from legal reform and legislative initiatives. It examines liability in a structured fashion by reference to conventional classifications of liability in contract, tort and criminal law. Each of these classifications is defined below, although the reader lacking in legal training is urged to recognize that the distinctions among the categories are not always clear.<sup>196</sup>

---

Locating a CA in the government may remove the incentive to mitigate exposure because a not-for-profit government agency does not seek the monetary rewards, or assume the financial risks, undertaken by private enterprise. To create an incentive for a government-operated FCA to function prudently, its employees probably need to face personal liability (both civil and criminal) for their acts. However, the possible benefits of this policy must be balanced against the disincentive thus produced for qualified and reliable personnel to accept positions.

<sup>195</sup> Cox v. Brookings Int'l Life Ins. Co., 331 N.W.2d 299, 303 (S.D. 1983).

Many organizations, both public and private, are subject to stringent internal and external audit oversight of their financial and other controls. If such organizations were to use FCA services, they could not satisfy their control requirements if they were required to state that the FCA undertook no liability for its actions. "A non-liaible FCA is of limited value for assuring security controls. The primary function of the FCA is to assume its users' 'identification risk' in free-form multilateral transactions. It therefore transfers and concentrates such risks in itself, in order to facilitate everyone else's interaction. If it does not assume this responsibility, the users will be better off reverting to bilateral or multilateral trading partner agreements, thereby forgoing the primary benefits of the public key infrastructure." Memo from F. Sudia (Nov. 16, 1993) (on file with Independent Monitoring).

<sup>196</sup> Grant Gilmore, Sterling Professor of Law, Yale Law School, has noted that:

. . . Classical contract theory might well be described as an attempt to stake out an enclave within the general domain of tort. The dykes which were set up to protect the enclave have, it is clear enough, been crumbling at a progressively rapid rate. With the growth of the ideas of

## Approaches to Apportionment of Liability

The following are common approaches to apportioning liability:<sup>197</sup>

- a. **Fault-based liability** - apportions liability based on determinations of fault in the context of the performance or non-performance of certain responsibilities.
- b. **Activity liability** - assigns liability based on the idea that any activity generates certain "accidental" costs that should be borne equally by those who initiate in the activity regardless of fault.

Liability can either be imposed by statutes and regulations establishing *per se* standards of conduct or by agreement. These approaches are subject to caveats, qualifications and complications, but would be useful to keep in mind during the following discussion.

In developing an appropriate approach to liability for the FCA, it is also useful to consider some of the rationales for the apportionment of liability. These include the following: *deep pocket* - the entity with the greatest financial resources should pay; *cheapest cost avoider* - the entity that can best minimize or eliminate the risk

---

quasi-contract and unjust enrichment, classical consideration theory was breached on the benefit side. With the growth of the promissory estoppel idea, it was breached on the detriment side. We are fast approaching the point where, to prevent unjust enrichment, any benefit received by a defendant must be paid for unless it was clearly meant as a gift; where any detriment reasonably incurred by a plaintiff in reliance on a defendant's assurances must be recompensed. When that point is reached, there is really no longer any viable distinction between liability in contract and liability in tort. We may take the fact that damages in contract have become indistinguishable from damages in tort as obscurely reflecting an instinctive, almost unconscious realization that the two fields, which had been artificially set apart, are gradually merging and becoming one.

G. GILMORE, THE DEATH OF CONTRACT 87-88 (1974).

<sup>197</sup> PROSSER & KEETON ON TORTS § 93 (5th ed. & Supp. 1988) [hereinafter PROSSER]. Prosser has also categorized "rules and practices [for] awarding and denying compensation as the fault principal, the strict accountability principle and the welfare principle." *Id.* § 85, at 608.



of harm should pay; *contribution* - liability should be apportioned as a function of the degree of fault; and *no fault* - the injured party bears its own loss.

Other policies sometimes displace the foregoing liability apportionments. Thus, the courts have implied exceptions to life insurance contracts "on the rationales of (1) preventing a wrongdoer from profiting from his or her criminal acts, (2) deterring crime, and (3) avoiding, or at least minimizing, the opportunities for fraud on insurers, as well as implementing the principle that insurance should not provide coverage when a loss is not fortuitous."<sup>198</sup>

---

<sup>198</sup> KEETON & WIDISS, *supra* note 16, § 5.3, at 477. At a much more detailed level, the following are sample apportionment schemes addressing data communications risks:

**Sender responsible.** The sender/offeror is the master of the communication. The message recipient has a duty to use the medium chosen by the sender/offeror, and is not involved in the document transfer until it retrieves the message from its service provider mailbox. However, the recipient generally has an obligation to check its mailbox and ensure that it is properly maintained.

**Recipient responsible.** The recipient, as the first person (positioned) to fully evaluate a message and determine whether it was properly communicated, is responsible for its accuracy. When the recipient questions the accuracy of a message, s/he can often download a copy of the message from the service provider, send an acknowledgment (a full copy or a functional acknowledgment) of the message as received to the sender, or otherwise use out-of-band mechanisms to further confirm the accuracy of the message.

**Sender and recipient jointly responsible.** When EDI is implemented for the mutual benefit of both trading partners, both parties should share the risks of EDI use. Each party to an EDI transaction generally receives some benefit from its use, and therefore apportionment of liability according to the direction of the communication (sender versus recipient) lacks merit.

**Sender or recipient responsible for choosing the service provider.** When one trading partner selects a particular service provider, that party should assume more responsibility for the service provider's performance.

**Each trading partner is unilaterally responsible for acts of its respective service provider.** Where each trading partner chooses its respective service provider, each party is in the best position to ensure its service



The legal implications of undertaking FCA activities or, more precisely, the liability implications of failing to perform them adequately, are legion. Because all participants, including users, will enter the FCA arena "voluntarily,"<sup>199</sup> the law of contracts is particularly important. Accordingly, this analysis commences with a discussion of certain issues respecting contract formation in the context of federally regulated activities and electronic communications generally. Next, because an extremely large portion of "FCA activities" (as defined in the preceding section) can be characterized as *certifications* (broadly defined) of relevant facts and circumstances, an inter-disciplinary treatment of liability issues respecting *certification* follows. Other civil liability issues, arising both within the law of contracts and tort, are next outlined and annotated with reference to specific FCA activities as appropriate. The analysis concludes with an examination of certain criminal liability issues.

A number of discrete legal issues have also been discussed in the foregoing survey. It should be noted at the outset that a considerable part of the following analysis is predicated upon the generic common law that would apply were all participants private entities. Special consideration of the liability of governmental entities and contractors is left to separate analysis in Section VII hereof.

## **B. Legal Infrastructure of the FCA**

As noted in Section V, the FCA will likely comprise a series of CAs, PCAs and a TLCA, arranged in hierarchical structures. Users who certify with one CA will likely wish to communicate with users who otherwise bear no direct relationship

---

provider's performance, in part because (1) the service provider is under a contractual obligation to provide a prescribed level of service to the trading partner and (2) status reporting and billing information is generally provided only to that trading partner.

ELECTRONIC CONTRACTING, *supra* note 2, § 2.22, at 74-76.

<sup>199</sup> The expression *voluntarily* is used advisedly. In legal comprehension, a *voluntary* act is one that is performed as the result of a conscious, volitional act, regardless of the practical or legal pressures necessitating it. Hence, one speaks of *voluntary* and *involuntary* petitions in bankruptcy: the former is filed *voluntarily* (often reluctantly) by the debtor himself; the latter is filed by disgruntled creditors. See 11 U.S.C. §§ 301, 303. Thus, the fact that the use of public key certificates may become a practical or legal requirement of commercial life, particularly in the area of government contracting, will not necessarily vitiate the *voluntary* contractual nature of the legal obligations arising in connection therewith.

with that CA or its PCA. There are two basic legal frameworks that might govern such a situation. The first is what we will call a "diffuse" infrastructure, in which users, CAs, and PCAs of the same hierarchy would be related to one another by a series of two-party interactions which would best be described as contractual in nature. Every participant would be a "stranger" in legal contemplation to every other participant not immediately above or below it in the hierarchy, as would be the case with every participant not a member of the same hierarchy.

The second infrastructure will be called "global." In it, the highest level member of any particular hierarchy would serve as the center of a single agreement or set of rules to which each member in the hierarchy would be a party and be bound. This might be accomplished with a contract to which each member would expressly agree upon, and as a condition to, entering the hierarchy. If the pinnacle were a federal, national entity, the "contract" might take the form of regulations; if an international entity, the form of a treaty among sovereign states.<sup>200</sup>

Not surprisingly, the United States banking system, which provides striking parallels to the FCA on several levels, exhibits varieties of most of the foregoing possibilities.<sup>201</sup> The following discussion addresses a number of contract formation issues in the FCA context.

Express contracts are those which contain "actual agreements of the parties, the terms of which are openly uttered or declared at the time of making it, being stated in distinct and explicit language, either orally or in writing."<sup>202</sup> A written agreement between the FCA and a user would be an example of an "express contract."<sup>203</sup> Written agreements are almost universally used among third-party

---

<sup>200</sup> The uncertainty and frankly optional nature of treaty obligations, and the variety among national laws, require that this possibility be explicitly considered only briefly. Most law world-wide recognizes concepts analogous to tort and contract and, absent rogue behavior on the part of sovereign states, the following analysis will bear considerable relevance to any international certification regime. See Section VII.A.5. ("International Organizations Generally"), *infra*.

<sup>201</sup> Thus, Article 4A of the U.C.C. contemplates a series of one-on-one transactions to effect wire transfers from one party to another. See Section VIII.A.2., *infra*. "Global" systems include CHIPS (contract) and Fedwire (regulation). See Sections VIII.A.4. and VIII.A.6., *infra*, on these systems respectively.

<sup>202</sup> BLACK'S LAW DICTIONARY 395 (4th ed. 1968).

<sup>203</sup> Although they will not be specifically addressed as part of the instant discussion herein, contracts *implied in fact* are those which are formed from conduct indicating an intention to be bound. For example, driving into a self-



service providers and users because providers believe that written agreements provide the highest level of certainty regarding important contractual issues, including the apportionment of liability.<sup>204</sup>

Contract enforceability requires the existence of formal elements, including most importantly, adequate specificity of terms and *consideration*.<sup>205</sup> Specificity of terms is provided by a sufficient *meeting of the minds* arrived at pursuant to the so-called "offer and acceptance" process. Recognizing that the FCA will desire practical and efficient procedures to bind its users, it may seek to use computer-based mechanisms for this purpose. For example, the FCA may wish to make a contract offer by promulgating terms in the Federal Register, publishing the terms in a user manual, or posting the terms on a computer bulletin board or in a computer-based directory. All participants will presumably wish assurances that the selected mechanism will satisfy contract formation requirements.

---

service gas station and filling one's tank implies an obligation to pay. The legal treatment of contracts implied in fact, apart from issues of evidence and proof which are unimportant for purposes of this paper, is identical to that of express contracts.

<sup>204</sup> See Section VIII.B. ("Value Added Network"), *infra*.

<sup>205</sup> The doctrine of consideration is among the most important and perplexing topics of the standard first-year law school curriculum. In essence, a party receives *consideration*, and is thereby contractually bound, when the other party performs some act, usually, but not always, at the request of the other party which he is not required by law to perform (such as the payment of money), or refrains from performing an act he is entitled to perform. Thus, if Party A promises to pay Party B a sum of money if B refrains from drinking and smoking for a period of time and B so refrains, A has received consideration and may be sued on his contractual obligation to pay the money. See *Hamer v. Sidway*, 124 N.Y. 538, 27 N.E. 256 (1891). In the latter part of the nineteenth century, courts for the most part ceased requiring the rough equivalence of each party's consideration, see HORWITZ, *supra* note 193, at 180-185, and the matter is currently a non-issue except when the rights of third parties such as creditors are at stake and within the context of the subjective doctrine of unconscionability. Fortunately, few of these issues will likely present problems given that commercial enterprises are envisioned to be the participants in a highly regulated industry and that FCA entities will undertake legal obligations in return for the payment of a fee (or series of fees) by users. On unconscionability generally, see note 346, *infra*.



"As a general proposition no contract can be formed unless the offeree knew of the offer at the time of his alleged acceptance."<sup>206</sup> An "offer must be so definite as to its material terms or require such definite terms in the acceptance that the promises and performances to be rendered by each party are reasonably certain."<sup>207</sup> The Federal Register is designed to communicate legally sufficient notice.<sup>208</sup>

The possibility of open, generic contracting has recently given rise to a controversy over whether it would or should be necessary for each user of the Federal Maritime Commission's Automated Tariff Filing and Information System (the "ATFI")<sup>209</sup> to execute a written and signed "User Agreement." The User Agreement, which was ultimately abandoned, would have granted users the right to access tariff information in its data base and imposed user fees, subject to various disclaimers.<sup>210</sup>

---

<sup>206</sup> J. CALAMARI & J. PERILLO, THE LAW OF CONTRACTS § 25 (1970) [hereinafter, CALAMARI].

<sup>207</sup> RESTATEMENT OF CONTRACTS (SECOND) § 32 (1981).

<sup>208</sup> See 5 U.S.C. § 552(a)(1).

<sup>209</sup> See 57 Fed. Reg. 36,248, 36,251 (Aug. 12, 1992); 58 Fed. Reg. 30,709 (May 27, 1993). The ATFI became operational on February 22, 1993.

<sup>210</sup> With respect to disclaimers, the proposed User Agreement provided:

ATFI data are provided "as is," without warranty of any kind, express or implied, including, but not limited to the warranties of performance, merchantability and fitness for a particular purpose. User shall make no claim(s) for damages relating to ATFI data. FMC's entire liability and the User's exclusive remedy shall be the replacement of any defective magnetic tapes which are returned to the FMC with a copy of the User's receipt. FMC has no liability whatsoever to User for any claim(s) relating in any way to:

(a) User's inability or failure to access or use data properly or completely; or

(b) Any lost profits, consequential, incidental or other special damages relating in whole or in part to User's rights hereunder or use of or inability to use data, even if FMC has been advised of the possibility of such damages.

User Agreement, Exhibit 2 to proposed 46 C.F.R. § 514, 58 Fed. Reg. 7504-7505 (Feb. 8, 1993). Interestingly, these disclaimers do not appear to have been replaced by the FMC's final regulation. See 58 Fed. Reg. 30,709.

The proposed User Agreement precipitated considerable public comment before being withdrawn. Perhaps the most interesting observation about the proposal's collective set of public comments was that the commenters did not directly question the underlying legal need for a user agreement to ensure that users are bound to the FMC's proposed terms. Rather, most commentators addressed the proposed agreement's substantive content. However, one commentator noted that the "User Agreement is a *contract of adhesion* [because users have] no opportunity to negotiate terms of the contract . . . and [are] presented [with it] . . . on a take-it-or-leave-it basis."<sup>211</sup> In the discussion accompanying its final regulation, the FMC stated, "In view of various commenters, the proposed User Agreement and/or various of its provisions . . . [are] abandon[ed]."<sup>212</sup>

Given the foregoing, it is likely that publishing FCA terms in the Federal Register and Code of Federal Regulations would satisfy contract formation requirements and such satisfaction is virtually certain where a subscriber signs on to a service with notice broadly stated of the existence of appended terms. An example of the latter is that of the Medicare program, pursuant to which hospitals and other health-care providers execute a one page or even one sentence agreement to the

---

It is not now currently planned for the AFTI to implement cryptographic methods for either authentication or confidentiality purposes. Telephone Interview with John Ewers, Deputy Managing Dir., ATFI, Washington, D.C. (Apr. 27, 1993). The reasons for the decision were that: (i) the FMC does not enter information into the system, (ii) it has implemented safeguards to prevent unauthorized information modification, and (iii) ATFI "[a]cceptance of tariff matter does not establish the legality of the rates and practices described therein." *Id.* (referencing 46 C.F.R. § 514.1(d)). When parties claim that there has been a "clerical error" in the data, the FMC urges that its Rules of Practice and Procedures are adequate to resolve both electronic and paper-based tariff filings. *Id.* (referencing 46 C.F.R. § 502).

<sup>211</sup> *In re: Filing of Tariffs and Service Contracts: Implementation of Section 502 of Public Law 102-582* (Docket No. 93-03), Comments of Transax Data at 6 (Mar. 10, 1993). On its own, the characterization "contract of adhesion" is of minimal legal import. See text accompanying note 346, *infra*. Billions of real world subscription transactions (for telephone service, transportation of passengers and freight, admission to a theater or parking lot) involve perfunctory acceptance of contracts of adhesion, some governed by tariffs, some not.

<sup>212</sup> 58 Fed. Reg. 30,709. It is difficult to tell whether the User Agreement concept was abandoned because it was thought unnecessary to accomplish its objectives and that regulation was otherwise adequate, or whether it was abandoned for political reasons on the mere pretext of legal disability.



effect that they agree to abide by the Medicare regulations "as in force from time to time." No case has been found in which the efficacy of such an arrangement was even challenged.

Accepted contractual conventions suggest that acceptance can be inferred from a use of the FCA in the context of clearly communicated terms: "Under the prevailing . . . test, [the offeree] will be held to what appeared from his expression to be his intention since the offeror has a right to rely upon this appearance, unless he knows or has reason to know that the offeree did not intend to accept."<sup>213</sup> In another view, "The beginning of performance by an offeree can be effective as acceptance so as to bind the offeror . . . if followed within a reasonable time by notice to the offeror."<sup>214</sup>

In general, computer-based mechanisms are probably sufficient to communicate offers and acceptances. For example, the Uniform Commercial Code states that "[u]nless otherwise unambiguously indicated by the language or circumstances . . . an offer to make a contract shall be construed as inviting acceptance in any manner and by any medium reasonable in the circumstances."<sup>215</sup> Computer-based acceptance of an offer to provide computer-related goods and/or services does not appear unreasonable in the abstract, and the clear trend is toward relying on these computer-based mechanisms for all communications purposes. This reliance seems natural given the widespread (and increasing) use of electronic data interchange and electronic mail, as well as the current and potential levels of trustworthiness of computer-based mechanisms. Accordingly, the FCA should not foreclose the option of developing computer-based mechanisms to automate appropriate aspects of contract formation.

Making FCA-certified digital signatures legally efficacious also raises issues regarding the enforceability and validity of "documents" digitally signed under the FCA's hierarchy and the evidentiary value of certificates and CRLs so signed in disputes between trading partners. Although the resolution of some of these issues is indispensable to the effectiveness of the FCA, they are largely beyond the scope of this Report, but have been addressed elsewhere.<sup>216</sup>

---

<sup>213</sup> CALAMARI, *supra* note 206, § 26; *see also* RESTATEMENT OF CONTRACTS (SECOND), *supra* note 207, at § 54.

<sup>214</sup> U.C.C. § 2-206, cmt. 3.

<sup>215</sup> U.C.C. § 2-206; *see* RESTATEMENT OF CONTRACTS (SECOND), *supra* note 207, § 30; *see also* ELECTRONIC CONTRACTING, *supra* note 2, § 6.8.

<sup>216</sup> *See* LINKING SECURITY, *supra* note 2, and citations therein. The trend toward greater recognition of computer-based acts, including those requiring signatures continues. *See, e.g.*, 58 Fed. Reg. 48,522 (Sept. 16, 1993) (modifying FCC rules to



It is indispensable that the FCA and its users become bound to the policies, rules of practice and other applicable rules that affect responsibilities and apportionment of liability. There will be a need to bring potentially thousands, and possibly millions, of users "up to speed." As the number of users increases, the execution of written agreements among all participants becomes less practical. There will also likely be instances where, by virtue of policy, "business decision," exigent circumstances or otherwise, no written agreement between users and the FCA will have been executed. In such cases, it is critical that all parties be assured that each other party is bound by contract or by public law.

As a legal matter, there would appear to be no general prohibition on the establishment of FCA-related contracts and such by non-written means. The Massachusetts statute of frauds, which is typical of those enacted in virtually every United States jurisdiction, requires a "writing" for the following types of contracts: agreements on the part of decedents' representatives to answer personally for decedents' debts; guaranties; agreements of marriage; agreements for the transfer of an interest in real property; agreements by a discharged debtor to pay his debts; agreements requesting wills; agreements for the sale of securities and agreements for certain brokerage contracts.<sup>217</sup>

The "statute of frauds" provision of the Uniform Commercial Code also requires a writing for contracts involving "transactions in goods having a value of more than \$500."<sup>218</sup> The federal government has been held liable on unwritten contracts,<sup>219</sup> and there would accordingly appear to be no bar on unwritten agreements from this quarter, in the absence of legislation to the contrary.

Another type of contract that typically requires a writing are those under which performance is not capable of being performed within a year.<sup>220</sup> Thus, if a user paid a fee for a certificate that would be valid for a period of two years, during which the issuer would, say, have a duty of responding to CRL requests and the

---

permit private radio "applications to be 'signed' by computer-generated impulses"); 58 Fed. Reg. 42,518 (Aug. 10, 1993) (announcing that DoD to modify billing procedures to permit carriers to "submit billings electronically").

<sup>217</sup> MASS. GEN. L. ch. 259, §§ 1, 3, 5-7 (1992 & Supp. 1993).

<sup>218</sup> U.C.C. § 2-201(a).

<sup>219</sup> The Tucker Act, 28 U.S.C. § 1491(a), confers federal jurisdiction over, *inter alia*, "any . . . implied contract with the United States . . ." The absence of a writing would appear to be a *sine qua non* of a contract implied in fact.

<sup>220</sup> See MASS. GEN. L. ch. 259, § 1.

like, the contract may well be within the Statute of Frauds. Courts are split as to whether an early termination provision is sufficient to remove a contract from the Statute of Frauds.<sup>221</sup> However, federal statutes or regulations preempt contrary state law pursuant to the Supremacy Clause of the United States Constitution,<sup>222</sup> and there would appear to be no basis to such preemption in the context of a *federal* certification authority.

Still, as a policy matter, the wisdom of using unwritten agreements is a different question altogether. Legislative and judicial institutions have been reluctant to impose the requirement of a writing in the absence of good cause for doing so. Thus, the law of insurance, for example, has considered the efficacy of oral insurance agreements and determined that:

[t]he disadvantages that could result from oral transactions for insurance have not been viewed as sufficiently compelling to warrant general statutory prohibitions that restrict or limit the enforceability of insurance commitments that have not been reduced to writing. Furthermore, despite some early dicta and occasional subsequent assumptions to the contrary, it is well established that there is no prohibition of decisional origin against oral contracts of insurance or oral binders.<sup>223</sup>

Notwithstanding the potential desirability or even necessity of non-written FCA agreements, their implications are broad. Thus, for example, dispensing with conventional writing altogether might result in an impaired (real or perceived) ability on the part of authorities to prosecute normatively criminal behavior.<sup>224</sup> These policy issues require careful consideration.<sup>225</sup>

---

<sup>221</sup> See CALAMARI, *supra* note 206, § 302.

<sup>222</sup> See U.S. CONST. art. 6, cl. 2.

<sup>223</sup> KEETON & WIDISS, *supra* note 16, § 2.2, at 45 (citing, *e.g.*, State Farm Mut. Auto. Ins. Co. v. Newell, 120 So.2d 390, 390 (Ala. 1960)). See generally Section IX.B. ("Insurance"), *infra*; LINKING SECURITY, *supra* note 2 (concerning the concept of a "writing").

<sup>224</sup> See Section VII.G. ("Criminal Liability"), *infra*. Note that the issue of criminal prosecution has been of particular concern to the Internal Revenue Service in the context of its electronic filing initiatives.

<sup>225</sup> Indeed, at least "higher assurance" FCA services will most likely require confidence in the success of criminal prosecution against law breakers and some criminal justice experts believe that written agreements will enhance prosecutorial success. Also, see Section IX.C., *infra* (concerning the use of written agreements for FCA purposes).



### C. CERTIFICATION LIABILITY

At the risk of tautology, it is argued that the FCA's primary function is *certification*, albeit defined in an especially broad fashion for purposes of this analysis. Indeed, it might also be argued that *certification* in this special sense is the principal FCA function that introduces novel challenges to the legal system.

The primary meaning of *certification*, of course, is the process that takes place when one presents credentials to the CA for purposes of obtaining a certificate. In theory, this is the point in time when identity is ascertained and bound to the public key embedded in a certificate. However, when the recipient of a communication verifies the purported originator's digital signature against certificates and applicable CRLs, another certification takes place – that none of an enumerated series of events has occurred and that the (original) certificate is valid. Moreover, this very process depends on yet another certificate: that of the CA (or CAs) maintaining or promulgating CRLs. These certificates are issued by PCAs, which also incidentally *certify* to one degree or another that their CAs perform their duties and maintain their systems in compliance with *policies*.<sup>226</sup> Again, PCAs and their policies are registered with, and/or certified by, hierarchically superior entities until, as some would have it, one reaches God.

The foregoing description leads to two extraordinarily useful simplifications. The first is that the entire system is built upon, and indeed is comprised of, nothing but a series of representations which either will or will not be adequately true (or carefully made) for the purposes of persons obtaining and acting in reliance upon them. The second simplification is a functional one. It consists of the fact that all certifications can be divided into two groups: (1) those that will be directly relied upon by *users* (i.e., that a public key is bound to a particular person, CA, PCA, etc. and that certain events have not occurred that would warrant its placement on a CRL) and (2) those that will be only implicitly or indirectly relied upon by users (all others).<sup>227</sup> The prior group will be referred to herein as "First-level Certifications," the latter as "Second-level Certifications."

The following analysis is structured around these two simplifications. It focuses on liability and remedies for *misrepresentation*, including the possibilities of

---

<sup>226</sup> See Section IX.C. (Policy Statements and Agreements), *infra*. This feature may comprise system testing and auditing functions. See also Section IX.A. ("Certification and Accreditation"), *infra*.

<sup>227</sup> By way of example, a user implicitly or indirectly relies upon PCA and perhaps higher certifications when he directly relies upon the contents of a CRL in assessing the authenticity of a given communication.



rights against those responsible in some manner for the misrepresentations of others. It also attempts to address the apparent complications generated by the fact that one may or may not be in *privity* with the various entities upon whose representations he is directly or implicitly relying.

## 1. Contract or Tort?

It has been recognized elsewhere that liability in contract and tort for mis-information can overlap in significant ways. Prosser writes, "Where economic harm [liability or misrepresentation] . . . results from the defendant's misfeasance, or from his nonfeasance plus reliance . . . [t]he promisor may be liable, either on a contract theory or tort theory or both, not only to the promisee, but also to those who are intended beneficiaries of the promise."<sup>228</sup> It is a guiding principle of this analysis that tort and contract, or both, often provide remedies for the same misrepresentation.<sup>229</sup>

## 2. First-Level Certification Liabilities

### a. Non-Certification

---

<sup>228</sup> PROSSER, *supra* note 197, § 93 (Supp. 1988).

<sup>229</sup> The decreasing relevance of *privity* (at one time an important limitation on contract remedies) has made itself manifest in other areas. Statutory relaxation of privity requirements in contract claims, *see, e.g.*, U.C.C. § 2-318, and the growth of tort law to fill gaps in the area of products liability has been cogently noted by one of the most intellectually respected commercial lawyers of modern times:

One of the most interesting case law developments of recent years . . . has been the expansion of a manufacturer's liability to remote users of his defective products -- the so-called "products liability" cases. The law of seller's warranty, it is true, has always had one foot in contract and one foot in tort. Gradually, it seemed, the contract side of warranty had prevailed; the successive codifications had dealt with warranties entirely in contract terms. Beginning in the mid-1950s the courts, unexpectedly reversing the long established and apparently settled allocation of warranty liability to contract, set out to fashion a new and much more expansive law of warranty based entirely in tort. Here again, I suggest, we see an almost instinctive choice of tort over contract as the principle of liability in a rapidly developing field.

GILMORE, *supra* note 196, at 92-93.

The often fictional notion that contracts are the product of voluntary arrangements implies the absence of a duty imposed by law to enter into them.<sup>230</sup> Thus, a CA would, in the absence of other considerations, face no liability for refusing to certify members of the public.

However, an ancient exception to this rule exists for so-called "common carriers," entities whose activities are deemed somehow "affected with the public interest." Such a "public interest" often arises by virtue of the importance or indispensability of an activity and/or of dominant market share for that activity.<sup>231</sup> A quintessential example of common carriers at common law are railroads.<sup>232</sup> It is logically feasible that a certification infrastructure operated entirely by private entities would find itself subject to common carrier duties, even without legislative intervention.<sup>233</sup> As noted by the Supreme Court nearly a century ago, "It is unnecessary to cite authorities to the proposition that it is the common law duty of the carrier to receive, carry and deliver goods . . . ."<sup>234</sup> Damages for violation of this duty would presumably be measured by lost profits,<sup>235</sup> if capable of proof, and in any event could include punitive damages.<sup>236</sup>

---

<sup>230</sup> At one time, "freedom of contract" was an exalted constitutional right. *See, e.g., Lochner v. New York*, 198 U.S. 45 (1905). That it is now accepted that the state may regulate this "freedom" to the virtual point of extinction is witnessed, for example, by the National Labor Relations Act, 29 U.S.C. §§ 141 *et seq.*: "Of course, the basic constitutionality of the . . . Act, as an exercise of the commerce power, is beyond question." *Int'l Brotherhood v. W.L. Mead, Inc.*, 230 F.2d 576, 579 (1st Cir. 1956) (citations omitted). However, in the absence of positive law to the contrary, this "freedom" remains intact.

<sup>231</sup> *See also* Section VIII.G. ("Common Carriers"), *infra*.

<sup>232</sup> *See, e.g., Wabash R.R. Co. v. Pearce*, 192 U.S. 179 (1904).

<sup>233</sup> Of course, common carrier duties may also be imposed by statute. *See, e.g.,* 49 U.S.C. § 11101(a) ("A common carrier providing transportation or services subject to the jurisdiction of the Interstate Commerce Commission . . . shall provide the transportation or services on reasonable request.").

<sup>234</sup> *Wabash R.R. Co.*, 192 U.S. at 187.

<sup>235</sup> *See, e.g., Johnson v. Chicago, M., S.P. & P.R.R.C.*, 400 F.2d 968, 975 (9th Cir. 1968).

<sup>236</sup> Various state and federal laws prohibit discrimination on the basis of factors such as race as well. However, these laws are applicable to business generally and like other such laws, will not be separately considered herein.

Common carrier or tariffed status is not always viewed as an unwelcome intrusion by private enterprise. It is often a means for gaining governmental immunity from competitive pressures, consumer pressures and fragmentary state-by-state or community-by-community regulation. It can also serve as a shield against tort liability.<sup>237</sup>

## **b. Misrepresentation by the User**

### **User v. CA**

Although liability on the part of a CA to an applicant<sup>238</sup> who misrepresents his identity is intuitively and legally unlikely, an important variation on the theme of "User misrepresentation" is the case of communications effected by an impostor with a private key that has been compromised. The degree to which a loss will be shared between the "true" (defrauded) User and the CA is not a problem unknown to the law. Clearly, the strength of the binding, the overall strength of the controls of the FCA and the use of signature tokens<sup>239</sup> must be considered in developing a workable solution to this problem.

The following simplified table is presented to consider the implications of the unauthorized use of an "authentication instrument" in analogous situations.

---

<sup>237</sup> See generally Section V.III.G. ("Common Carriers"), *infra*.

<sup>238</sup> Applicants who obtain certificates are hereinafter referred to as "Users."

<sup>239</sup> See Section IV.L. ("Use of Card Technologies"), *supra*.



Authentication Instrument	User Liability for Misuse
Notarial Seal	Ordinary negligence <sup>240</sup>
Credit Card	Strict liability but limited to \$50 <sup>241</sup>
Hand Stamp	Comparative negligence <sup>242</sup>
Bank Card PIN	Strict liability limited to \$50 with timely notice of loss/theft <sup>243</sup>

**TABLE 1 - LIABILITY FOR UNAUTHORIZED USE OF AUTHEN. INSTRUMENT**

### **Recipient v. CA – Tort Liability**

The recipient ("Recipient") of a communication who suffers a loss as the result of reliance upon a fraudulent certificate may have various avenues of relief against the CA. As will be the case generally throughout this analysis, those avenues of relief will depend to a large degree on whether a "diffuse" or "global" legal infrastructure is in place.

In a diffuse infrastructure, the Recipient will most likely not have a contractual relationship with the CA. Accordingly, his remedies are likely to be limited to those arising in tort, namely the law of negligent misrepresentation. Liability for negligent misrepresentation arises in the following manner:

One who, in the course of business, profession or employment . . . supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he

<sup>240</sup> See Sections VI.E. and VIII.D., *infra*.

<sup>241</sup> See 15 U.S.C. § 1643(a) (discussed *infra* Section VIII.A.7.).

<sup>242</sup> See U.C.C. § 3-406 (precluding assertion of forgery against payor bank when drawer negligent in contributing to signature except when bank also negligent). Prior to revision in 1990, Article 3 gave a complete defense, by way of contributory negligence, to the bank. See U.C.C. § 3-406 (pre-revision). See generally Section VIII.A.1., *infra*.

<sup>243</sup> See 15 U.S.C. § 1693g (discussed *infra* Section VIII.A.3.). Whether the card issuer will be able to shift its loss back to the merchant is principally a matter of contract. Typically, the issuer will bear the loss unless the card appeared on a restricted card list or the merchant demonstrably failed to compare signatures, such as when it neglected to obtain that of the purchaser. See H. SCOTT, MATERIALS ON COMMERCIAL LAW: THE PAYMENT SYSTEM 279-80 (Harvard Law School, Winter 1993).

fails to exercise reasonable care or competence in obtaining or communicating the information.<sup>244</sup>

A significant restriction upon liability is that the provider of the false information must know or have reason to know that the recipient will rely upon it.<sup>245</sup> This should not be an impediment in the FCA context because maintaining a directory or releasing certificates to Recipients clearly puts them within this class. Moreover, limitations of liability in CA-User contracts would not be binding on those, such as Recipients, not party to them.

The principal conceptual issue in a claim for negligent misrepresentation would be the exercise of reasonable care or competence. In the absence of cases or guidelines defining a CA's duty of care in ascertaining a person's identity, the duty can be described with little certainty. However, a court would likely find the standard of care imposed on notaries public<sup>246</sup> or the regulatory standards for the issuance of passports<sup>247</sup> to be persuasive. These standards would not necessarily be determinative, however, and to the extent a party argues that FCA functions should be subject to a higher or lower standard a court would be free to apply such a standard. To the extent the FCA is deemed to be a common carrier (as previously discussed), it will most likely be held to a higher standard of care.

Another possibility for the CA's "duty of care" is that of strict liability. Courts have imposed liability for harm caused regardless of fault or lack thereof on entities engaged in certain conduct which includes, but is not limited to, "abnormally dangerous" activities.<sup>248</sup> Abnormally dangerous activities typically involve the use of explosives, the harboring of wild animals and the like, while certification merely facilitates (usually peaceful) commerce and communication. However, such liability is usually confined to non-economic injuries (such as personal injury). In the economic loss and property loss realm, there is, among other things, the strict liability of "bailees" in certain circumstances.<sup>249</sup>

---

<sup>244</sup> RESTATEMENT OF TORTS (SECOND) § 552(1).

<sup>245</sup> *See id.* § 552(2). However, the element of reliance on the information may not be comparably necessary under a general negligence or professional negligence theory.

<sup>246</sup> *See* Section VIII.D. ("Notaries Public"), *infra*.

<sup>247</sup> *See* Section VIII.F. ("Department of State"), *infra*.

<sup>248</sup> RESTATEMENT OF TORTS (SECOND) § 519.

<sup>249</sup> *See* Section VIII.C.3. ("Bailor-Bailee Relationship"), *infra*, for a separate discussion of the rules of bailment.



## Recipient v. CA -- Contract Liability

In a "global" infrastructure, of course, the Recipient would have contractual rights against the CA. However, because contracts could contain a substantial variety of provisions on this issue, one can only speculate as to what rights might be provided. In general, liability under a contract is "strict": the defendant either has or has not performed. Thus, a CA's liability for user misrepresentation under an FCA contract containing a provision along the lines of, "The CA shall ascertain the identity of Users and certify same to Recipients upon request of Recipients" might be strict. However, it is more likely for FCA contracts to provide for the use of "due care," "best efforts," or "reasonable efforts" on the part of the CA. Litigation over such a provision would resemble that which would pertain in a negligence suit. Finally, there is evidence in the cases that contracts for the professional provision of services contain "implied warranties" of professional competence and diligence.<sup>250</sup> These warranties, however, are of *skill* only. Favorable results are only warranted as a matter of express contract.<sup>251</sup> On the other hand, it has been held that certain implied warranties may *not* be disclaimed, at least in the consumer context.<sup>252</sup>

In the unlikely event that first-level certification activities were considered to be a "transaction in goods," the Uniform Commercial Code (the "U.C.C.") would impose additional contractual duties.<sup>253</sup> Moreover, the U.C.C. provisions on disclaimers of warranties and limitations on liability are likely to be highly persuasive to courts scrutinizing such clauses whether or not the U.C.C. "governs" as a formal matter.

---

<sup>250</sup> See, e.g., *Data Processing Servs. Inc. v. L.H. Smith Oil Corp.*, 492 N.E.2d 314 (Ind. App. 1986) (computer programming). The concept is not new, and appears in 3 W. BLACKSTONE, COMMENTARIES 163-64 (repr. 1966) (1768).

<sup>251</sup> See *Chemical Bank v. Title Servs. Inc.*, 708 F. Supp. 245, 247 (D.Minn. 1989). Compare the definition of "assurances" in Section III, *supra*.

<sup>252</sup> See *Melody Home Mfg. Co. v. Barnes*, 741 S.W.2d 349, 355 (Tex. 1987). Note also that the Magnuson-Moss Act, 15 U.S.C. §§ 2301 *et seq.* and state laws such as Mass. Gen. L. ch. 93A place strict limitations on the disclaimer of implied warranties. Compare the U.C.C.'s treatment of this issue at Section VI.D., *infra*.

<sup>253</sup> See Section VI.D. ("General Contract Liability Considerations"), *infra*.



## Other

Other forms of User misrepresentation or related actionable conduct may arise to the extent that the CA contract requires the reporting of certain events to the CA (such as a compromise of a private key or a change in critical information, *e.g.*, removal of a User's authority to represent his employer), which the User fails to perform. CA liability to a Recipient in this case is unlikely unless strict liability or a duty to monitor the status of Users is imposed by statute or "global" contract.

### c. Misrepresentation by the CA

CA misrepresentation would create liability exposure both to Users and to Recipients. CA misrepresentation may be divided into four categories:

- failure to include certificates in a directory or other failure to make them available to would-be Recipients;
- inaccurate publication of certificates;
- failure to observe a duty to place certificates on a CRL; and
- wrongful placement of certificates on a CRL.<sup>254</sup>

It should be noted at the outset that, in addition to traditional theories of recovery in tort or contract, such "sloppy" conduct or practices might expose CAs to Federal Trade Commission ("FTC") Act<sup>255</sup> and "baby FTC Act"<sup>256</sup> liabilities.

### User v. CA -- In Contract

Given that the certificate application process has been posited to be of a contractual nature, CA liability to Users for its misrepresentations will, with certain important exceptions, be governed by the terms of the contract between them. Again, because there is no FCA contract yet in existence, determining the scope of a CA's liability is speculative. Nonetheless, certain observations may be

---

<sup>254</sup> Hereinafter, the act of placing a certificate on a CRL will be referred to as "listing" it.

<sup>255</sup> 15 U.S.C. §§ 41 *et seq.*

<sup>256</sup> See, *e.g.*, MASS. GEN. L. ch. 93A; *Midland Mgt. Corp. v. Computer Consoles Inc.*, No. 87-C-0971 (N.D. Ill. Aug. 16, 1993) (holding Illinois baby FTC Act applicable to computer performance dispute and awarding attorneys' fees).

advanced. First, the considerations appearing above<sup>257</sup> respecting contracts would generally apply equally to CA liability as to Users. Second, various kinds of CA misrepresentations bear close relationships to other areas of the law. For example, if the CA were to permit communications to be "certified" by the appearance of inaccurate certificates in a directory or failing to list certificates, Users could conceivably become unexpectedly bound to contracts with Recipients by virtue of what amounts to a misrepresentation of identity by the CA. The issue here is whether the CA is the *agent* of the User such that the CA may bind the User with its acts.

Agency is a critical concept in liability law. Actual or apparent authority to act as an agent results in the putative principal's being bound by the agent's actions and imposes certain duties which, if not properly discharged, could result in liability for the agent. The question of whether a messaging intermediary can be considered the agent of a sender arose as a consequence of the development of the telegraph in the early nineteenth century. A noted authority on contract law considers the situation in which a telegraph company introduced error into a transmission by slightly changing the price of the goods and notes the conflicting law on this point. Ultimately, it is decided that a relationship of agency does not exist:

Again, it may be said that the sender of the telegram has chosen the telegraph company as his agent, thus making it appear that some general rule of agency can be deductively applied. While it is true that the sender of a telegram knows that it must be translated by the clerks into a telegraphic code and back into words, with some possibility of error in the process, this is hardly enough to establish a relation of agency. Assuredly, the sender does not hold out the telegraph clerk as his agent with power to contract on his behalf. Nor is the clerk his servant. The telegraph company is a public servant, much like the post office . . . under compulsion to serve all comers and to bear the responsibility that accompanies public service.<sup>258</sup>

---

<sup>257</sup> See *supra* ("User Misrepresentation: Recipient v. CA - Contract"). It is conceivable for remedies to exist in negligence and contract in the event a contractual duty is negligently performed.

<sup>258</sup> 1 A.L. CORBIN, CORBIN ON CONTRACTS § 105 (1963); see also *Butler v. Foley*, 179 N.W. 34 (Mich. 1920) (considering a contract based on three telegrams where the defendant contended that the telegraph company was the plaintiff's agent for purposes of risk of error in transmission of the defendant's reply); Whitter, *Restatement of Contracts and Mutual Assent*, 17 CALIF. L. REV. 441, 447-448 (1929); Cf. *Western Union Tel. Co. v. Cowin & Co.*, 20 F.2d 103 (8th Cir. 1927) (holding that telegraph company is an independent contractor responsible to both the sender and receiver for errors). See generally PROSSER, *supra* note 197, § 3.10(4), at 250 (considering claims against common carriers).



Similar questions are now being discussed by TPSPs and their users, discussions which on occasion have led to specific agreements.<sup>259</sup> Although the contractual rules of TPSPs and clearing houses often expressly disclaim agency relationship,<sup>260</sup> the FCA might potentially be considered an agent of the user if it were intimately involved in electronic contract formation on behalf of users. Moreover, it should be noted that disclaimers of agency relationships would be of little or no avail against Recipients under a "diffuse" legal infrastructure. To the extent a User suffers loss to a Recipient in consequence of CA misconduct as "agent," the User would presumably be permitted to seek indemnification or contribution from the CA.<sup>261</sup>

Various forms of CA misrepresentation bear other similarities to established law. Failure to list a revoked certificate is closely analogous to failure to observe a "stop-payment" order on a check. Similarly, wrongful listing of a certificate is closely analogous to "wrongful dishonor" of a check. In crafting User-CA contracts, or in the event of absence or ambiguity of relevant provisions therein, the liability allocation schemes of Article 4 of the Uniform Commercial Code are relevant and warrant consideration.<sup>262</sup>

---

<sup>259</sup> See Section VIII.B. ("Value Added Networks"), *infra*.

<sup>260</sup> See *id.*; see also Section VIII.A., *infra* (discussing electronic payment systems). However, consider that "[p]ersons or business entities employed for a single transaction or a series of transactions can be agents, even though as to their physical activities, they demean themselves as independent contractors." *Rosenstein v. Standard & Poor's Corp.*, 1993 WL 176532 (Ill. App. May 26, 1993) *appeal denied*, 622 N.E.2d 1227 (Ill. 1993) (citing *Protective Ins. Co. v. Coleman*, 494 N.E.2d 1241 (Ill. App. 1986)). *Rosenstein* upheld an exculpatory clause of a licensing agreement and that was incorporated into an exchange's clearing house rules against a claim of negligent misrepresentation (erroneous stock closing price) "[e]ven where a semi-public nature is found to permeate the transaction between the parties. . . ." *Id.* at \*6-\*7 (restating the courts "reluctan[ce] to find any special or social relationship that would obviate the impact of an exculpatory clause.").

<sup>261</sup> See H. REUSCHLEIN & W. GREGORY, *THE LAW OF AGENCY AND PARTNERSHIP* §§ 70 *et seq.* (2d ed. 1990).

<sup>262</sup> See Section VIII.A.1., ("U.C.C. Articles 3 and 4 (Checks)") *infra*.



## User v. CA – In Tort

As noted above, a User's remedies in tort against the CA for misrepresentation will largely be superseded by its remedies in contract. This state of affairs stems from the pervasive use and legal enforceability of so-called "merger" or "integration" clauses.<sup>263</sup> In the event the certification process were deemed a "transaction in goods," considerable authority exists for the proposition that the enactment of the Uniform Commercial Code precludes negligence claims for "mere" economic loss.<sup>264</sup> Nonetheless, "[p]roof of fraud in the inducement may . . . enable the [User] to avoid the warranty disclaimers and parol evidence rule . . . . Moreover, actionable fraud will vitiate contractual limitations on the [User's] remedy and right to recover consequential and other damages."<sup>265</sup>

The elements of fraudulent misrepresentation are satisfied when a person makes:

- 1) a misrepresentation or a concealment of a material fact;
- 2) who knew or should have known that the representation was false;
- 3) who intended for the representation to be relied on;
- 4) where the representation was justifiably relied on; and
- 5) the user suffered damages as a result of reliance on the misrepresentation.<sup>266</sup>

Although *puffing* (statements, typically of a promotional character, which do not amount to assertions of material fact) is not typically actionable, the novelty and

---

<sup>263</sup> See Friedman & Hildebrand, *Computer Litigation: A Buyer's Theory of Liability*. Application of the "parol evidence rule" will preclude one party's proof of a provision that is inconsistent with the written agreement. In commercial cases, a "blanket disclaimer or a finding of integration will generally negate any parol warranties." *Earman Oil Co. v. Burroughs Corp.*, 625 F.2d 1291, 1298 (5th Cir. 1980).

<sup>264</sup> See, e.g., *MESA Business Equip., Inc. v. Ultimate S. Cal., Inc.*, 931 F.2d 60 (D. Cal. 1993) (citing *Seely v. White Motor Co.*, 45 Cal. Rptr. 17, 23 (1965)); *Tokio [sic] Marine & Fire Ins. Co. v. McDonnell Douglas Corp.*, 617 F.2d 936, 941 (2d Cir. 1980); *S.M. Wilson & Co. v. Smith Int'l. Inc.*, 587 F.2d 1363 (9th Cir. 1978), *aff'd without opinion*, 931 F.2d 60 (9th Cir. 1991).

<sup>265</sup> Friedman & Hildebrand, *supra* note 263 (citing *Glovatorium v. NCR Corp.*, 684 F.2d 658 (9th Cir. 1982); see also *Clements Auto Co. v. Service Bureau Corp.*, 444 F.2d 169 (8th Cir. 1971)).

<sup>266</sup> See PROSSER, *supra* note 197, § 105, at 728; see also RESTATEMENT OF TORTS (SECOND) § 525.

level of trustworthiness required of FCA activities suggests that the courts may grant little leeway for puffing.<sup>267</sup>

The courts have found a number of fraudulent misrepresentations concerning the provision of computer-based products.<sup>268</sup> The FCA would be particularly vulnerable if it knowingly misrepresented the certification or listing process as sufficient to meet a given User's security requirements. Importantly, in a suit for fraud or misrepresentation, evidence of conversations the parties had before the contract was entered into would be admissible. This evidence would otherwise be superseded by an integration clause in a contract, and its admissibility would tend to benefit one of the parties.<sup>269</sup> Also, a contractual limitation precluding recovery of consequential damages will not apply to a claim for fraudulent misrepresentation.<sup>270</sup>

### Recipient v. CA -- Contract

The liability in contract of a CA to a Recipient under a "global" legal infrastructure has been discussed above in connection with "User Misrepresentation."<sup>271</sup> Even in a "diffuse" infrastructure, however, the Recipient may be able to assert rights

---

<sup>267</sup> Cf. *Sierra Diesel Injection Serv. v. Burroughs Corp.*, 651 F. Supp. 1371, 1378 (D. Nev. 1987) (misrepresentation that a computer system would satisfy accounting requirements).

<sup>268</sup> See, e.g., *Accusystems, Inc. v. Honeywell Info. Sys., Inc.*, 580 F. Supp. 474, 482 (S.D.N.Y. 1984) (holding false statements that new system had been extensively tested and could concurrently perform multiple tasks for multiple users to be fraudulent); *Triangle Underwriters, Inc. v. Honeywell, Inc.*, 604 F.2d 737, 746-48 (2d Cir. 1979) (misrepresentation in fraudulent inducement claim); *Sierra Diesel Injection Serv.*, 651 F. Supp. 1371; *Computer Sys. Eng'g, Inc. v. Qantel Corp.*, 571 F. Supp. 1365, 1367, 1372-73 (D. Mass. 1983), *aff'd*, 740 F.2d 59 (1st Cir. 1984) (holding that false inducement to purchase or lease computer prod. is actionable); *Walter Raczynski Product Design v. IBM*, No. 92-C-6423 (N.D. Ill. July 20, 1993) (misrepresentations concerning future conduct).

<sup>269</sup> See *Financial Timing Publications, Inc. v. Compugraphic Corp.*, 893 F.2d 936 (8th Cir. 1990).

<sup>270</sup> See *APLications Inc. v. Hewlett-Packard Co.*, 501 F. Supp. 129 (S.D.N.Y. 1980), *aff'd* 672 F.2d 1076 (2d Cir. 1982); *Clements Auto Co. v. Service Bureau Corp.*, 444 F.2d 169, 188-89 (8th Cir. 1971).

<sup>271</sup> See *supra* "User Misrepresentation: Receipt v. CA-Contract."



against the CA as a "third-party beneficiary" to the User-CA contract. In general, third-party beneficiary rights arise under a contract between two other persons pursuant to which the obligor is to render performance to the third party.<sup>272</sup> An outmoded means of analyzing third-party beneficiary situations was to permit the beneficiary to enforce performance or to seek damages of the promisor (here, the CA) only if it were a "creditor" beneficiary (to whom the promisee owed a pre-existing duty that would be discharged by performance) or a "donee" beneficiary (on whom the promisee intended to confer a gift in the form of performance).<sup>273</sup> Under this analysis, a Recipient would have third-party beneficiary rights only if the User and the Recipient were operating under a relationship pursuant to which the User had an obligation to provide certification (here, actionable assurances) of its identity, non-repudiation, or the like.<sup>274</sup>

The "modern" approach, in contrast, requires only that the putative third-party beneficiary be an "intended" beneficiary of the promisor's performance.<sup>275</sup> This approach is manifested in the explosive growth of "third-party" liability. The most notorious facet of this trend exists in the causes of action asserted against accountants and bankers in securities fraud lawsuits. Some states have acted legislatively to limit the liability of accountants and other professionals to persons who are not their clients.<sup>276</sup> Although the "intended beneficiary" formulation

---

<sup>272</sup> See generally CALAMARI, *supra* note 206, §§ 243-244, at 378-384.

<sup>273</sup> *Id.* § 244, at 379-80 (citing, *e.g.*, RESTATEMENT OF CONTRACTS (FIRST) § 133 (1932)).

<sup>274</sup> We may pass over the "donee beneficiary" theory of liability in that the possibility that a (commercial) User would seek to confer a "gift" on a Recipient by means of using certified methods of communication is a trivial one.

<sup>275</sup> CALAMARI, *supra* note 206, § 240, at 380-384 (citing, *e.g.*, RESTATEMENT OF CONTRACTS (SECOND) § 133 (Tentative Draft, 1964)). Incidentally, the Second Restatement's final version, which appeared in 1981, placed the doctrine's discussion at § 302.

<sup>276</sup> See, *e.g.*, Seamons, *Third Party Liability Under the Illinois Public Accounting Act*, 81 ILL. B.J. 256 (1993). In Illinois, for example, accountants are shielded from liability "to persons not in privity of contract," except in cases of fraud or intentional misrepresentation or when the accountant is "aware" that a primary intent of the client was for the professional services to benefit or influence the particular person bringing the action and which person has received notice from the accountant manifesting its awareness of the prospective reliance. Seamons *supra*, at 256-57 (discussing 255 ILCS 450/30.1 (1992)). Cf. *Central Bank of Denver v. First Interstate Bank of Denver*, 114 S. Ct. 1439 (1994) (holding that the Securities and Exchange Act of 1934, § 10(b) does not cover private action aiding and abetting



would presumably continue to govern situations in which the User is contractually required to provide certification for its communications, conceptual difficulties arise in the absence of such a pre-existing obligation. More particularly, it is difficult to determine in the abstract and in the utter absence of analogous case law or doctrine whether certification of a User's identity and communications constitutes the conferral of a benefit on, or the running of performance to, the User or the Recipient. A court could plausibly reach either result, and CA liability to Recipients under a third-party beneficiary theory can only be suggested as a distinct, but by no means certain or even probable, possibility.

### Recipient v. CA -- Tort

In terms of liability in tort to Recipients, the CA will, of course, continue to be responsible for negligent misrepresentations.<sup>277</sup> However, the introduction to the analysis of a degree of fault on the part of the CA adds two new possibilities for liability: negligent non-feasance (*e.g.*, failing to make certificates available to potential Recipients) and fraudulent or intentional misrepresentation.<sup>278</sup>

Although a party ordinarily faces no liability in tort for mere failure to act,<sup>279</sup> liability for "non-feasance" can arise when the party is under an obligation to perform, such as when the party itself has created the circumstances putting another in danger.<sup>280</sup> Moreover, even when a person is under no obligation to perform an act, he must perform that act, if undertaken, with ordinary care.<sup>281</sup> Accordingly, a CA could face liability to Recipients in tort for both non-feasance and mis-feasance in connection with the certification process.<sup>282</sup>

---

liability suit under the Act's general antifraud provision; attorneys not a "suspect class".).

<sup>277</sup> See text accompanying notes 546-551, *infra* (concerning misrepresentation under the Federal Tort Claims Act).

<sup>278</sup> Fraudulent misrepresentation is discussed at Section VI.C.2.c. ("Misrepresentation by the CA": "User v. CA -- In Tort"), *supra*.

<sup>279</sup> See, *e.g.*, R. POSNER, THE PROBLEMS OF JURISPRUDENCE 350 (1990).

<sup>280</sup> See *id.* (citing cases).

<sup>281</sup> See *id.* (citing *Farwell v. Keaton*, 240 N.W.2d 217 (Mich. 1976)).

<sup>282</sup> "Negligent misfeasance" would presumably be comprised within the foregoing discussion of "negligent misrepresentation." Potential manifestations

Negligence is recognized as having four elements:

1. A duty, or obligation, recognized by the law, requiring the person to conform to a certain standard of conduct, for the protection of others against unreasonable risks.
2. A failure on the person's part to conform to the standard required: a breach of the duty. . .
3. A reasonably close causal connection between the conduct and the resulting injury. This is what is commonly known as "legal cause," or "proximate cause," and which [presupposes] the notion of "cause in fact."
4. Actual loss or damage resulting to the interests of another.<sup>283</sup>

The *failure* required by the negligence standard with respect to information technology may require more than a programming or similar error in the absence of strict liability.<sup>284</sup> Although a higher standard of care in a case has been applied in cases where the software provider was familiar with the user's particular requirements.<sup>285</sup>

A duty is defined, for negligence purposes, "as an obligation, to which the law will give recognition and effect, to conform to a particular standard of conduct toward another."<sup>286</sup> As already noted, the duty owed (whether in negligence, strict liability or any other theory) by a CA to its participants, including the class of Recipients to whom a duty is owed, is a pivotal issue and one without clear boundaries. To the extent that the duty owed in computer-related cases has been expanding, the FCA is likely to inherit that expansion. The majority view is that a duty is owed to the "group of persons for whose benefit and guidance [the FCA]

---

of negligent misrepresentation could include, *e.g.*, failure to correctly handle or maintain CRLs, "certificate holds" (where applicable) or perhaps even a failure to perform identification. CAs involved in certifying parties to high value/risk transactions may, depending on the facts, be held to a particularly high standards.

<sup>283</sup> PROSSER, *supra* note 197, § 30, at 164-165.

<sup>284</sup> See *Georgetown Science and Arts, Ltd. v. Microsystems Eng'g Corp.*, Civ. Act. No. 81-0422 (D.D.C. Feb. 29, 1984). The court noted that "programs [do] not ordinarily run perfectly when initially developed and . . . it is quite normal to have a shakedown period to test, debug and modify programs to achieve the objectives of a client." *Id.* at 343. However, the software industry has matured since this 1984 decision and may be held to a higher standard.

<sup>285</sup> See *Leson Chevrolet Co., Inc. v. Oakleaf & Assoc., Inc.*, 796 F.2d 76 (5th Cir. 1986)).

<sup>286</sup> PROSSER, *supra* note 197, § 53, at 356.



intends to supply the information. . . ."<sup>287</sup> It is perfectly possible that courts will define the class to whom a duty is owed as all foreseeable FCA Recipients for purposes of negligent non-feasance.

"Good faith" on the part of the FCA is unlikely to mitigate its liability for negligent non-feasance. Even early computer law cases held that good faith reliance on computer-generated errors did not insulate actors from their negligence. In one case, the court noted that:

[The defendant] explains that this whole incident occurred because of a mistake by a computer. Men feed data into a computer and men interpret the answer the computer spews forth. In this computerized age, the law must require that men in the use of computerized data regard those with whom they are dealing as more important than a perforation on a card. Trust in the infallibility of a computer is hardly a defense, when the opportunity to avoid the error is as apparent and repeated as was here presented.<sup>288</sup>

### 3. Second-Level Certification Liabilities

#### a. Direct Liability in Tort or Contract

As noted above, "second-level" certification activities are defined for purposes of this analysis to include representations on the part of a "superior" member in a hierarchy that the members constituting one or more subordinate levels do or will do certain things or act or will act with a certain level of care.<sup>289</sup>

Quintessential "second-level certifications" appear in the PCA Policy Statements reproduced herein as Appendix E.<sup>290</sup>

---

<sup>287</sup> RESTATEMENT OF TORTS (SECOND) § 552(2)(a).

<sup>288</sup> *Ford Motor Credit Co. v. Swarens*, 447 S.W.2d. 53 (Ky. 1964); *cf. Thompson v. San Antonio Retail Merchant's Ass'n*, 682 F.2d 509, 513 (5th Cir. 1982) (social security number of applicant put in wrong data file of credit company's computer data base resulting in erroneous credit history).

<sup>289</sup> A general analysis of the importance and functions of "second-level certifications" appears generally as Section VI.C.3., *supra*.

<sup>290</sup> Various "second-level" certifications therein include the following: "[This policy] is intended for [CAs] . . . using identification criteria which are reasonable," Appendix E.3. ("T.I.S."), *infra*, at ¶ 2; "It is expected that each CA . . . will make a good faith effort . . . to protect its private key against disclosure," *id.* at ¶ 3. See generally *RSA Data Security Inc., Certificate Services, An RSA White Paper* (July 15, 1993) (describing RSA's Commercial Certificate Hierarchy and the basis for certain of its corresponding policies).



An entity making such certifications faces liability for fraudulent or negligent misrepresentation to the extent such statements turn out not to have been warranted and affirmative misconduct or breach of a duty of care is proven.<sup>291</sup> Cases concerning the liability of Underwriters Laboratories and similar organizations for negligent certification of the products of others exist<sup>292</sup> and, because they are factually similar to a second-level certification case, cannot be disregarded. On the issue of Recipient reliance, availability of policies to Recipients and the "hedging" language they contain, if any, would be important. Finally, in a "global" infrastructure, a second-level certifier is likely to be able to prescribe its duties and potential liabilities to all other parties to a substantial degree. However, as will be discussed below, these provisions are not always enforceable.

### **b. Vicarious Liability**

For policy reasons, the law occasionally places liability on one entity for the acts of another irrespective of the former's fault. In the commercial arena, this usually occurs in one of two situations: when a party's "agent" (*e.g.*, an employee) breaches a duty of care that causes harm, and when a party's "independent contractor" causes harm in the course of performing an unreasonably dangerous activity, regardless of fault.<sup>293</sup> The difference between an "agent" and an

---

<sup>291</sup> Arguably, liability can expand to other torts as well.

<sup>292</sup> See *Hampstead v. General Fire Extinguisher Corp.*, 267 F. Supp. 109 (D. Del. 1969) (holding Underwriters Laboratories ("UL") liable for exploding extinguisher if (i) approval was negligent, (ii) purchaser relied on approval, (iii) purchaser belonged to a protected, foreseeable class, and (iv) purchaser would not have brought extinguisher but for UL approval); *Hanberry v. Hearst Corp.*, 81 Cal. Rptr. 519 (1969) (Good Housekeeping's Consumer Guarantee Seal concerning slippery shoes). *But cf.* *Benco Plastics, Inc. v. Westinghouse Elec. Corp.*, 387 F. Supp. 772 (E.D. Tenn. 1974) (citing "practical policy grounds," including (i) lack of privity with injured party, (ii) nonphysical nature of injury, (iii) problematic causation, (iv) lack of evidence of reliance (v) low moral culpability of UL, (vi) UL's policy of preventing future harm, and (vii) the nature of endorser's business).

<sup>293</sup> "Strict" liability for "abnormally dangerous activities" is discussed above, at Section VI.C.2.b., and below at Section VIII.G.3. (concerning dangerous goods handed over to the operators of transport terminals). It is argued there that certification activities are unlikely to be deemed "abnormally dangerous." Again, however, the possibility is noted herein. See also Section IX.B., *infra* (concerning insurance issues associated with inherently dangerous activities).

"independent contractor" is essentially a matter of the degree of control exercised over its conduct.

Hence if, for example, a negligent CA were determined to be an "agent" of a PCA, the PCA would be "vicariously" liable for the negligent acts of its agent, the CA. Whether an entity being certified by a PCA, TLCA, or the like is the certifier's "agent" is a question of fact that cannot be determined on the basis of a situation not yet in existence. A contractual right on the part of the certifier, for example, to dislodge management and to exercise direct control as opposed to a right merely to terminate the contract and/or to seek damages, could be strong evidence of an agency relationship. Also, in a "diffuse" legal infrastructure, mere disclaimers of agency status would not be binding on Recipients and other entities who are not parties to the contract containing the disclaimers.

## D. GENERAL CONTRACT LIABILITY CONSIDERATIONS (INCLUDING DAMAGES)

### 1. Applicability of the U.C.C.

Article 2 of the Uniform Commercial Code applies to transactions in (particularly sales of) *goods*.<sup>294</sup> The principal consequences in liability terms of the U.C.C.'s applicability to the FCA concern warranties and limitations of liability. Because of the multiplicity of potential FCA activities, it is possible for some (and perhaps all) of them to be covered by this uniform body of state law.<sup>295</sup> Two questions must be answered in order to determine the U.C.C.'s applicability to a given FCA-related activity: whether the transaction is a "sale" of "goods." As a formal matter, the U.C.C. defines "sale" as "the passing of title from the seller to a buyer for a price,"<sup>296</sup> but essentially empties this construct of meaning by later providing: "Each provision of this Article with regard to the rights, obligations and remedies of the seller, the buyer, purchasers or other third parties applies irrespective of title to the goods except where the provision refers to such title."<sup>297</sup> The U.C.C.'s elevation of substance over form has been articulated in cases holding "leases" of personal property and the granting of communications licenses, for example, to be *sales*.<sup>298</sup>

The U.C.C. defines goods as "things which are movable at the time of identification to the contract for sale . . . ." <sup>299</sup> In the context of information

---

<sup>294</sup> See U.C.C. § 2-102.

<sup>295</sup> For example, the FCA might provide software which would be used to generate key pairs and/or applications for storing, processing and using certificates; it might also offer hardware such as card technologies to hold key pairs, to generate digital signatures, or to provide other forms of secured access and communications.

<sup>296</sup> U.C.C. § 2-106(1).

<sup>297</sup> *Id.* § 2-401.

<sup>298</sup> See, e.g., *Patriot Gen. Life Ins. Co. v. CFC Inv. Co.*, 420 N.E.2d 918, 922 (Mass. App.Ct. 1981); see also U.C.C. § 1-201(37) (distinguishing "true" leases from "leases intended as security"). On licenses, see, e.g., *Communications Groups, Inc. v. Warner Communications Inc.*, 527 N.Y.S.2d 341, 344-45 (Civ. Ct. 1988); *RXX Industries, Inc. v. Lab-Con, Inc.*, 722 F.2d 543, 546-47 (9th Cir. 1985). Cf. *In Re Koreag, Controle et Revision S.A.*, 961 F.2d 341 (2nd Cir. 1992), *cert. denied*, 113 S.Ct. 188 (1992) (foreign exchange held to be a good under Article 2).

<sup>299</sup> U.C.C. § 2-105(1).



technology, courts have held that various computer-related products may be considered goods, and the U.C.C. has been held to apply to user-vendor disputes in which both hardware and software sales are considered "transactions in goods."<sup>300</sup> In *RRX Industries v. Lab-Con, Inc.*, for example, the court found the purchase of a software system to be a transaction in goods rather than the provision of services.<sup>301</sup> If the transaction combines the sale of goods and the provision of services, the analysis must go further and determine whether goods or services predominate.<sup>302</sup>

For example, computer-based directory services have been considered *goods* for certain purposes, and any directory services the FCA provides might fall into this category.<sup>303</sup> While neither the simple omission of a subscriber from a phone

---

<sup>300</sup> See, e.g., *Advent Sys. Ltd. v. Unisys Corp.*, 925 F.2d 670 (3d Cir. 1991). For a case involving integrated hardware and software, see *Chatlos Sys., Inc. v. National Cash Register Corp.*, 635 F.2d 1081 (3d Cir. 1980), *cert. denied*, 457 U.S. 1112 (1982) *But see* *Geotech Energy Corp. v. Gulf States Telecommunications and Info. Sys., Inc.*, 788 S.W.2d 386 (Tex. Ct. App. 1990) ("essential" nature of services rendered made "sale" of computerized phone system *not* a transaction in goods). Data processing services, including computerized analysis, collection, storage and reporting of data are historically not subject to U.C.C. applications, *but see* *The Colonial Life Insur. Co. v. Electronic Data Sys. Corp.*, 817 F. Supp. 235 (D. N.H. 1993) (data processing contract was sale of goods); *cf.* *Computer Servicenters, Inc. v. Beacon Mfg. Co.*, 328 F. Supp. 653, 655 (D. S.C. 1970), *aff'd.*, 443 F.2d 906 (4th Cir. 1971) (contract for performance of data processing services not "sale of goods").

<sup>301</sup> 772 F.2d 543 (9th Cir. 1985); *see also* *Systems Design & Management Information, Inc. v. Kansas City Post Office Employees' Credit Union*, 788 P.2d 878 (Kan. App. 1990) (software development); *Wharton Mgt. Group v. Sigma Consultants, Inc.*, No. 89C-JA-165 (Del. Super. Ct. Jan 29, 1990), *aff'd.*, 582 A.2d 936 (Del. 1990) (custom-developed software is generally considered a service); *Software Licenses Communications Group, Inc. v. Warner Communications Inc.*, 527 N.Y.S. 2d 341 (1988).

<sup>302</sup> See, e.g., *Neibarger v. Universal Co-Operatives, Inc.*, 386 N.W.2d 612 (Mich. 1992); *St. Ann-Nackawic Pulp Co., Ltd. v. Research-Cottrell, Inc.*, 788 F. Supp. 729 (S.D.N.Y. 1992). The court in *MESA Business Equip., Inc. v. Ultimate S. Cal., Inc.*, 931 F.2d 60 (D.Cal. 1993), stated that "when a sale predominates, incidental services provided do not alter the basic transaction. Because software packages vary depending on the needs of the consumer, we apply a case-by-case analysis." *Id.* at 2-3 (quoting *RRX*, 772 F.2d at 546).

<sup>303</sup> See, e.g., *Hawaiian Tel. Co. v. Microform Data Sys., Inc.*, 829 F.2d 919 (9th Cir. 1987) (computer-based directory services).

directory, nor the refusal to distribute a rectification before the publication of the following year's directory, is generally considered sufficiently serious to result in significant damages, "in the case of the electronic telephone directory, subscribers should find it easier to obtain compensation even in the area of administrative law, since in this case any error can easily be corrected at the subscriber's request - so that this kind of error should no longer be permitted."<sup>304</sup>

It should also be kept in mind that there are proposed reforms to the U.C.C. which may diminish the distinctions between sales and services in the case of computer software contracts.<sup>305</sup>

## 2. Warranties Under the U.C.C.

### Express Warranties

The U.C.C. provides an important set of rules concerning express warranties. Even in situations where the U.C.C. does not govern formally, these rules are likely to be highly persuasive or even to exert sufficient force that they are deemed declaratory of the common law. A "warranty" is an assurance by one contracting party of the existence of a fact upon which the other party may rely. It is intended to relieve the promisee of any duty to ascertain the fact for himself, and amounts to a promise to indemnify the promisee for any loss if the fact warranted proves untrue.<sup>306</sup> The U.C.C. defines express warranties in detail.<sup>307</sup>

---

<sup>304</sup> J. Huet, *Product Liability In The Information Field*, in INTERNATIONAL CONTRACTS FOR SALE OF INFORMATION SERVICES 157, 166 (1988).

<sup>305</sup> See, e.g., R. Nimmer & R. Speidel, *Hub and Spoke Concepts in Article 2: Discussion Memorandum* (Sept. 5, 1993) (on file with Independent Monitoring) (reflecting "a recognition of various forces that are reshaping commercial contract practices and the proper relationship between those developments and the basic commercial contract law contained in Article 2."). *Id.* at 3.

<sup>306</sup> See *Micro-Managers, Inc. v. Gregory*, 434 N.W.2d 97, 101 (Wis. Ct. App. 1988).

<sup>307</sup> Under the U.C.C., express warranties are created by:

- (a) Any affirmation of fact or promise made by the seller to the buyer which relates to the goods and becomes part of the basis of the bargain creates an express warranty that the goods shall conform to the affirmation or promise.



The words "warranty" or "guarantee" need not be used to create an express warranty<sup>308</sup> and a warranty may include descriptions<sup>309</sup> and advertisements.<sup>310</sup> The typical types of express warranties that appear in information technology-related agreements (and which vendors often try to disclaim) include "freedom from defects in material and workmanship" for hardware, and "performance substantially in accordance with specifications" for software.

### Disclaimer of Express Warranties

When the FCA contracts to provide FCA-related services, it will likely seek to limit or exclude express warranties explicitly. However, there are certain limitations on disclaiming express warranties. First, "[s]ince a product's performance forms the fundamental basis for a sales contract, it is patently unreasonable to assume that a buyer would purchase a standardized mass product from an industry seller without any enforceable performance standards."<sup>311</sup>

---

(b) Any description of the goods which is made part of the basis of the bargain creates an express warranty that the goods shall conform to the description.

(c) Any sample or model which is made part of the basis of the bargain creates an express warranty that the whole of the goods shall conform to the sample or model.

§ 2-313(1).

<sup>308</sup> See *id.* § 2-313(2) ("It is not necessary to the creation of an express warranty that the seller use formal words such as 'warrant' or 'guarantee' or that he have a specific intention to make a warranty, but an affirmation merely of the value of the goods or a statement purporting to be merely the seller's opinion or commendation of the goods does not create a warranty."); see *USM Corp. v. Arthur D. Little Sys., Inc.*, 546 N.E.2d 888 (Mass. App. 1989) (interpreting broadly express warranty for a "turnkey" systems, despite effective general disclaimers of the implied warranties of merchantability and fitness for a particular purpose); *Chatlos Sys., Inc. v. National Cash Register Corp.*, 479 F. Supp. 738, 743 (D.N.J. 1979), *aff'd on liability and remanded on damages*, 635 F.2d 1081 (3d Cir. 1980), *cert. denied*, 457 U.S. 1112 (1982) (verbal representations of seller).

<sup>309</sup> See *APLications Inc. v. Hewlett-Packard Co.*, 501 F. Supp. 129 (S.D.N.Y. 1980), *aff'd*, 672 F.2d 1076 (2d Cir. 1982) (technical brochures).

<sup>310</sup> See *Overstreet v. Norden Lab., Inc.*, 669 F.2d 1286, 1290 (6th Cir. 1982) (catalog description or advertisement).

<sup>311</sup> *A&M Produce Co. v. FMC Corp.*, 186 Cal. Rptr. 114, 125 (Ct. App. 1982).



Second, disclaimers of express warranty must not be unconscionable.<sup>312</sup> Accordingly, technical compliance with the U.C.C. does not ensure enforceability of the disclaimer.

Integration or merger clauses<sup>313</sup> (which purport to exclude prior written or oral agreements) are another means of disclaiming express warranties in certain circumstances, such as when the express warranty is claimed to have been made outside of the contract itself.<sup>314</sup> The buyer's sophistication and knowledge of warranties are relevant to assessing the effectiveness of merger clauses. Although the issue of unsophisticated users does not seem applicable to this Report's conception of FCA liability,<sup>315</sup> the question arises as to who is considered a "sophisticated" user in this context, in that, with respect to the FCA's novel and complex products and potential use of electronic contracts, users experienced in

---

<sup>312</sup> See note 346 below on unconscionability.

<sup>313</sup> The U.C.C. provides with respect to merger clauses as follows:

Terms with respect to which the confirmatory memoranda of the parties agree or which are otherwise set forth in a writing intended by the parties as a final expression of their agreement with respect to such terms as are included therein may not be contradicted by evidence of any prior agreement or of a contemporaneous oral agreement but may be explained or supplemented

- (a) by course of dealing or usage of trade . . . or by course of performance . . . ; and
- (b) by evidence of consistent additional terms unless the court finds the writing to have been intended also as a complete and exclusive statement of the terms of the agreement.

U.C.C. § 2-202. This section will most likely be revised in the redrafting process underway by the Nat'l Conf. of Comm'rs on Uniform State Laws.

<sup>314</sup> In this regard, a brochure was effectively disclaimed by an integration clause in a contract. *See APLlications Inc. v. Hewlett-Packard*, 672 F.2d 1076, 1077 (2d Cir. 1982). In California, when a non-demurrable cause of action for misrepresentation is stated along with a cause of action for breach of warranty, oral testimony concerning precontract representations is admissible despite the existence of an otherwise valid integration clause in the license agreement. *See id.*

<sup>315</sup> See text accompanying notes 31 and 960, *supra* (assumptions and recommendations concerning consumers, respectively).

forming regular contracts may (at least initially) become relatively "unsophisticated" when dealing with the FCA.

An understanding of the distinctions the courts have made in the ability to enforce integration clauses against various classes of users is important. An integration clause will generally exclude express warranties outside of the contract in the absence of evidence of a specific intent to create such a warranty. If the seller makes an affirmation merely of the value of the goods or makes a statement "purporting to be merely the seller's opinion or recommendation of the goods," then an express warranty has not been created.<sup>316</sup> For the FCA, this may mean that statements concerning the general level of authentication or trust associated with using the FCA may not create an express warranty, although the FCA will likely be held to a reasonably high standard.

### Implied Warranties

In addition to the creation of express warranties, various "implied warranties" also arise upon a sale of goods unless they have been effectively disclaimed.

As previously discussed, it is not perfectly clear that FCA activities will not be considered transactions in "goods" (with the corresponding influence of U.C.C.-style warranty law, or lack thereof). In addition, trends in recent case law suggest that the traditional exclusion of services is narrowing.<sup>317</sup> Consequently, attention should be given to two forms of implied warranty imposed under the U.C.C.: those of *merchantability* and of *fitness for a particular purpose*.<sup>318</sup>

The implied warranty of merchantability is treated as follows:

- (1) Unless excluded or modified . . . a warranty that the goods shall be merchantable is implied in a contract for their sale if the seller is a merchant with respect to goods of that kind. . .
- (2) Goods to be merchantable must be at least such as
  - (a) pass without objection in the trade under the contract description; and
  - (b) in the case of fungible goods, are of fair and average quality within the description; and
  - (c) are fit for the ordinary purposes for which such goods are used; and
  - (d) run, within the variations permitted by the agreement, of even kind, quality and quantity within each unit and among all units involved; and

---

<sup>316</sup> U.C.C. § 2-313(2).

<sup>317</sup> See text accompanying note 305, *supra*.

<sup>318</sup> Other implied warranties include those of title and non-infringement. See U.C.C. § 2-312.



- (e) are adequately contained, packaged, and labeled as the agreement may require; and
  - (f) conform to the promise or affirmations of fact made on the container or label if any.
- (3) Unless excluded or modified other implied warranties may arise from course of dealing or usage of trade.<sup>319</sup>

The implied warranty of fitness for a particular purpose is stated in the U.C.C. to apply as follows:

Where the seller at the time of contracting has reason to know any particular purpose for which the goods are required and that the buyer is relying on the seller's skill or judgment to select or furnish suitable goods, there is unless excluded or modified under the next section an implied warranty that the goods shall be fit for such purpose.<sup>320</sup>

Arguments supporting the applicability of the implied warranty of fitness for a particular purpose to the FCA include:

- The information contained in certificate applications arguably puts the FCA on notice of particular purpose(s) for which the certificate is to be used. For example, charge the FCA with knowing the name of the user (*e.g.*, the XYZ Bank) and therefore the probable nature of its business (*e.g.*, financial services).
- Most FCA users will rely on the FCA's judgment and expertise, which arguably is the point of its existence. Many written comments submitted in response to the proposed Digital Signature Standard FIPS revealed a lack of user sophistication and knowledge of cryptography, as well as the assumption (whether by design or default) that, for example, "NIST knows best."
- Warranties of fitness for a particular purpose may significantly affect the CA if the CA is charged with knowledge of the importance of the transactions that it facilitates. This knowledge could increase the damages the FCA would have to pay were it to breach its implied warranty of fitness for a particular purpose.

Whether these arguments justify the applicability of an implied warranty of fitness for a particular purpose is yet to be determined.

---

<sup>319</sup> *Id.* § 2-314; *see Neilson Business Equip. Ctr., Inc. v. Monteleone*, 524 A.2d 1172, 1175 (Del. 1987) (failure to perform record- and book-keeping rendered computer system unmerchantable).

<sup>320</sup> U.C.C. § 2-315.



## Disclaimer of Implied Warranties

Given the potential reach of implied warranties, it is important to determine whether the FCA will be able to limit or exclude them:

The reluctance of common law to imply warranties in service contracts can be explained by the fact that service contracts usually envision continuing performance on both sides of the contract, but many sales of goods are complete once the goods are delivered.<sup>321</sup> When continuing performance is called for on both sides, consumers have a self-help remedy available: they can stop payment if the services do not meet their expectations.

Regardless of legal right, the leverage available to the victim of disappointed expectations is substantial in an on-going relationship. Moreover, because the supplier performs over a period of time, any deficiency in the services supplied is likely to be detected before the supplier performs further. This reduces the possibility of forfeiture in the event of a breach that is less than total.<sup>322</sup>

However, a doctrinal difficulty with the foregoing traditional analysis is that a breach in many service agreements, including, perhaps in particular, FCA contracts, could potentially cause such extensive short-term harm that the impact of *on-going relationships* on the traditional analysis is or should be weakened.

Section 2-316(3) provides three alternatives for disclaiming implied warranties:<sup>323</sup> use of an express disclaimer or the term "as is" or the like; opportunity on the part of the buyer to inspect the goods, to the extent that such inspection would have resulted in the discovery of defects; and course of dealing and trade usage. Among the three, only the first is truly reliable as a planning device. A disclaimer of implied warranties must be made in a "conspicuous" manner if in writing, and disclaimer of the merchantability warranty must mention the term "merchantability."<sup>324</sup> There is a reluctance to uphold disclaimers in "form," or

---

<sup>321</sup> Citing, *inter alia*, RESTATEMENT (SECOND) OF CONTRACTS § 237. Note that the reference to on-going relationships would theoretically apply to the FCA even if its products were considered goods and not services; the key is whether, in fact, the relationship is presumed to be on-going.

<sup>322</sup> ELECTRONIC CONTRACTING, *supra* note 2, § 9.9, at 521.

<sup>323</sup> See U.C.C. § 2-316(3); *see also id.* § 2-316(2) (allowing exclusion of warranties of merchantability and fitness).

<sup>324</sup> *Id.* § 2-316(2). Other federal and state laws govern the applicability and disclosure of implied warranties. In *Sierra Diesel Injection Serv., Inc. v. Burroughs Corp.*, 874 F.2d 653, 658 (9th Cir. 1989), the court stated that "[w]hether a disclaimer is conspicuous is not simply a matter of measuring the type size or looking at the placement of the disclaimer within the contract. A reviewing court must ascertain that a reasonable person in the buyer's position would not have

"boilerplate," contracts when an unsophisticated user did not read the disclaimer before the purchase.

### 3. Remedies

Liability in contract can be described generally as arising from breach of its terms. Contract interpretation is a science unto itself and, like constitutional interpretation, is often a matter of philosophy or taste. However, once the terms have been determined, the principal question remaining is whether they have been followed:<sup>325</sup>

A breach of contract occurs where it is found that the promisor is under an absolute duty to perform, and that this absolute duty of performance has not been discharged, then this failure to perform in accordance with contractual terms will amount to a breach of the contract. In general, a breach must be material in order for it to give rise to damages to the injured party. A material breach is one where the promisee did not receive the substantial benefit of the bargain as a result of the failure to perform or because of defective performance by the promisor.<sup>326</sup>

*Materiality* constitutes an important limitation on the availability of remedies for breach of contract: it is often said that the law does not concern itself with trivial matters. Thus, if two parties have a contract to be performed on a certain day or at

---

been surprised to find the warranty disclaimer in the contract." Cf. *MESA Business Equip., Inc. v. Ultimate S. Cal., Inc.*, 931 F.2d 60, 63-64 (D.Cal. 1993) (holding that disclaimer need not be conspicuous when purchaser knows of its existence).

Certain courts may effectively require a warranty disclaimer to be expressly negotiated. "The battle of the forms", see U.C.C. § 2-207, can also result in the loss of warranty disclaimers. See *Arizona Retail Sys., Inc. v. The Software Link, Inc.*, 1993 WL 339860 (D. Ariz. July 27, 1993) (contractual limitations imposed by shrink-wrap license); *Step-Saver Data Sys. v. Wyse Technology*, 939 F.2d 91 (3d Cir. 1991).

<sup>325</sup> There is an overlap between a negligence theory derived from a contract-based duty and a simple breach of contract theory. Under the U.C.C., breach of contract is often a matter of "no-fault" liability. "We well appreciate that [strict tort liability] is often indistinguishable from liability for breach of the implied warranty of merchantability." WHITE & SUMMER, UNIFORM COMMERCIAL CODE 271 (1972). U.C.C. § 2-314 (concerning the implied warranty of merchantability) "offers a form of strict liability." *Id.* at 286.

<sup>326</sup> RESTATEMENT (SECOND) OF CONTRACTS § 241.



a certain time and performance is slightly delayed, no remedy will lie unless time was *of the essence*. The presumption is that time is *not* of the essence:

It is a general principle governing the construction of contracts that stipulations as to the time of their performance are not necessarily of the essence, unless it clearly appears in the given case from express stipulations of the contract or the nature of its subject-matter that the parties intended performance within the time fixed in the contract to be a condition precedent to its enforcement.<sup>327</sup>

In the case of FCA activities, the "nature of [the] subject-matter" is reliable and virtually instantaneous use of certification in furtherance of information transfers. In general, timeliness will be an important aspect of FCA performance and, accordingly, an untimely transfer will in many cases amount to a material breach. However, this is one of the many issues that should be dealt with by express agreement or regulation.

A plaintiff must prove the existence of a material breach and that the plaintiff is not in breach in order to be awarded remedies for breach of contract. More than one remedy may apply depending on the facts and applicable rules.<sup>328</sup>

#### **a. Direct Damages**

Direct damages are intended to return the non-breaching party to the condition that would have existed had the contract been performed. In most cases, the damages award will be based on an "expectation" measure, which is the value of what the non-breaching party would have gained had the contract been performed. This usually amounts to damages sufficient for the plaintiff to obtain a substitute performance.<sup>329</sup>

---

<sup>327</sup> Beck & Pauli Lithographing Co. v. Colorado Milling & Elevator Co., 52 F. 700 (8th Cir. 1892).

<sup>328</sup> See RESTATEMENT (SECOND) OF CONTRACTS § 347; cf. U.C.C. § 2-719(1)(b) ("[R]esort to a remedy as provided is optional unless the remedy is expressly agreed to be exclusive, in which case it is the sole remedy.").

<sup>329</sup> See RESTATEMENT (SECOND) OF CONTRACTS § 347. Costs associated with the use of cryptographic methods, which could also serve as a basis for comparison in attempting to calculate for damages resulting from FCA misconduct, are surveyed in LINKING SECURITY, *supra* note 2.

The following is a list of various damages which have been found compensable in computer user-vendor cases:

- Transportation charges



The following restates the generic formula for expectation damages:

- a. The loss in expected value of the other party's performance caused by the failure or deficiency thereof; plus -
- b. Any other loss, including incidental loss, caused by the breach; less -
- c. Any cost or other loss avoided as a result of the breach including contract termination.

## **b. Consequential Damages**

Liability for *consequential* damages can also be viewed as a separate and distinct problem. These damages include, typically, lost profits, loss of reputation, or loss of business opportunity.<sup>330</sup> The law has disfavored (and imposed limitations on)

- 
- Insurance charges (shipment and ongoing)
  - Repair costs -- parts
  - Maintenance and service charges
  - Taxes
  - Room preparation costs (rewiring, remodeling, air-conditioning)
  - Increased labor costs (clerical, programmers)
  - Training costs for employees
  - Percentage of executive salaries for time spent on computer system
  - Conversion costs
  - Business losses/lost profits (excessive inventory, lost sales, lost profits, liability to third parties, damages to business reputation, lost receivables)
  - Cost of space occupied by computer
  - Cost of supplies for computer
  - Cost of additional equipment and maintenance due to computer
  - Finance charges incurred in acquisition of computer

L. Reece, *Computer Liability: Where Have We Been and Where Are We Going?* Twelfth Annual New England Computer Law Conference 388-389 (Boston, May 1992).

<sup>330</sup> If the FCA undertakes to perform generalized communication services, and it fails to deliver a message that would have resulted in a large profit to the sender, that lost profit could serve as a measure of consequential damages. Compensatory damages, on the other hand, would consist only of the sender's expenses in directing the message by another route and the like. Cf. text accompanying note 1103, *infra* (beginning of section on common carriers).

the concept of consequential damages since at least the time of *Hadley v. Baxendale*,<sup>331</sup> in which the court held that a contractor could not be held liable for consequential damages because the other party had not notified the former of special circumstances pursuant to which a delay would cause lost profits. The concept continues to exert considerable influence, as evidenced by the noted case of *Evra Corp. v. Swiss Bank Corp.*<sup>332</sup>

*Hadley* stands for the general proposition that only reasonably foreseeable damages can be recovered.<sup>333</sup> The question of FCA liability for consequential damages requires resolution because consequential damages could potentially result in limitless exposure. The *Evra* case provides a good example of this danger for computer-based intermediaries in the funds transfer industry:

The success of the wholesale wire transfer industry has largely been based on its ability to effect payment at low cost and great speed. Both of these essential aspects of the modern wire transfer system would be adversely affected by a rule that imposed on banks liability for consequential damages. A banking industry amicus brief in *Evra* stated: "Whether banks can continue to make EFT services available on a widespread basis, by charging reasonable rates, depends on whether they can do so without incurring unlimited consequential risks. Certainly, no bank would handle for \$3.25 a transaction entailing potential liability in the millions of dollars."<sup>334</sup>

*Evra* considered the extent of a bank's liability for failure to make a transfer of funds when requested by wire to do so, which failure resulted in cancellation of plaintiff's ship charter. The plaintiff sued to recover certain related legal expenses plus profits that it had lost upon cancellation. Recovery of consequential damages tends to be fact specific, as *Evra* indicates:

---

<sup>331</sup> 156 Eng. Rep. 145 (1854) (delayed delivery of mill shaft resulting in lost profits).

<sup>332</sup> 673 F.2d 951 (7th Cir. 1982); *see also* *Underground Constr. Co. v. Sanitary Dist.*, 11 N.E.2d 361, 365 (Ill. 1937); *Western Union Tel. Co. v. Martin*, 9 Ill. App. 587, 591-93 (1882); *Siegel v. Western Union Tel. Co.*, 37 N.E.2d 868, 871 (Ill. App. 1941) (defendant not liable for profits that would have been obtained had funds been delivered in a timely fashion to permit legal bet because it lacked knowledge of purpose for transmittal); *Spangler v. Holthusen*, 61 Ill. App. 3d 74, 80-82, 278 N.E.2d 304, 309-10 (1978).

<sup>333</sup> *See* *Neering v. Illinois Cent. RR. Co.*, 50 N.E.2d 497, 503 (Ill. 1943) (tort damages limited to foreseeable consequences of defendant's carelessness). Only foreseeable damages are recoverable in contract as well. *See* RESTATEMENT (SECOND) OF CONTRACTS § 351 (1979).

<sup>334</sup> U.C.C. § 4A-305 cmt. 2; *see also* Section VIII.A.2., *infra*.



Swiss Bank failed to comply with the payment order, and no transfer of funds was made to the account of the [ship's] owner . . . . No one knows exactly what went wrong. One possibility is that the receiving telex machine had simply run out of paper, in which event it would not print the message although it had received it. Another is that whoever took the message out of the machine after it was printed failed to deliver it to the banking department. Unlike the machine in the cable department that the Continental telex operator had originally tried to reach, the machines in the foreign exchange department were operated by junior foreign exchange dealers rather than by professional telex operators, although Swiss Bank knew that messages intended for other departments were sometimes diverted to the telex machines in the foreign exchange departments.<sup>335</sup>

Judge Posner, who is known for his application of economic principles to legal issues, noted that the plaintiff was a sophisticated business enterprise that "should have known that even the Swiss are not infallible; that messages sometimes get lost or delayed in transit . . . ." <sup>336</sup> In essence, the court was working under a foreseeability analysis that implicated the level of care Swiss Bank owed: "The amount of care that a person ought to take is a function of the probability and magnitude of the harm that may occur if he does not take care."<sup>337</sup> The court continued:

To estimate the extent of its probable liability in order to know how many and how elaborate fail-safe features to install in its telex rooms or how much insurance to buy against the inevitable failures, Swiss Bank would have to collect reams of information about firms that are not even its regular customers . . . . These were circumstances too remote from Swiss Bank's practical range of knowledge to have affected its decision as to who should man the telex machines in the foreign department or whether it would have more intelligent machines or should install more machines in the cable department, any more than the falling off a platform scale because a conductor jostled a passenger who was carrying fireworks was a prospect that could have influenced the amount of care taken by the Long Island Railroad.<sup>338</sup>

---

<sup>335</sup> *Evra*, 673 F.2d at 953.

<sup>336</sup> *Id.* at 957.

<sup>337</sup> *Id.* at 958 (citing *U.S. v. Carol Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947); *Bezark v. Kostner Manor, Inc.*, 172 N.E.2d 424, 426-27 (1961)); *see also* *U.S. v. Consolidated Edison Co. of N.Y.*, 590 F. Supp. 266 (S.D.N.Y. 1984) (when a utility did not adequately test a new system that resulted in computerized overbilling, defendant was held liable for \$100,000 in interest).

<sup>338</sup> *Evra*, 673 F.2d at 958. (citing *Palsgraf v. Long Island R.R.*, 248 N.Y. 339, 162 N.E. 99 (1928).



*Evra* concluded by noting that "the kind of general foreseeability, which is present in virtually every case, does not justify an award of consequential damages."<sup>339</sup> In other words, everything is generally foreseeable to the extent that anything is possible. But this sense of foreseeability is excessively broad, in the *Evra* court's view, as a legal standard. The probability and extent of harm must also be taken into account.

Whereas the mishap in *Evra* stands as an example of what is not reasonably foreseeable, another "electronics" case gives examples of damages that would be foreseeable: "[d]estruction of data and the attendant consequences of erroneous invoices, lost or misshipped orders, bizarre product substitutions, lost goodwill and morale, as well as lost profits, are just the type of damages one would expect when a complex software system . . . malfunctions."<sup>340</sup> In this regard, the FCA may be held liable for consequential damages when it is charged with knowing the user's particular contingencies. Ascertaining the FCA's knowledge of given contingencies is a question of fact.

Another basis, this time statutory in nature, for the allowance of consequential damages involves, *bad faith*. For example, consequential damages for loss of a check are precluded unless the bank acted in bad faith.<sup>341</sup>

---

<sup>339</sup> *Id.* at 959. The general standard for foreseeability is as follows: Any loss that the party in breach "did not have reason to foresee as a probable result of the breach because it follows from the breach (a) in the ordinary course of events, or (b) as a result of special circumstances beyond the ordinary course of events, that the party in breach had reason to know is considered unforeseeable." RESTATEMENT (SECOND) OF CONTRACTS § 351.

<sup>340</sup> *Analysts Int'l Corp. v. Recycled Paper Prods., Inc.*, 1987 WL 12917 (N.D. Ill. Oct. 7, 1987).

<sup>341</sup> See U.C.C. § 4-103(5).

### c. Specific Performance

A non-breaching party may seek specific performance of the contract where other legal remedies are inadequate: "A non-breaching party may seek specific performance if it can be shown that enforcement is feasible and that mutuality of remedy is present, meaning that if the breaching party had wanted to do so, the other party could have enforced the contract against the party seeking specific performance."<sup>342</sup>

The FCA might be held to specific performance because the courts may find that the services provided by the FCA are "unique."<sup>343</sup> For example, if there were only one CA, there would be no alternative to securing relevant services at the hand of the CA and specific performance would likely be warranted. However, specific performance would be of little help to the user subsequent to certain kinds of irrevocable breach. The contract or regulation governing the FCA might, for instance, require the CA to issue the user a new certificate (FCA key issuance is, of course, generally not recommended). This sort of specific performance, however, would not necessarily undo damage already done to the user.

### d. Rescission, Restitution and Reliance Damages

Contract rescission, or cancellation, is a fairly straight forward concept: "Cancellation occurs when either party puts an end to the contract for breach by the other and its effect is the same as that of 'termination' except that the canceling party also retains any remedy for breach of the whole contract or any unperformed balance."<sup>344</sup> Restitution also involves both sides returning any consideration received. It is an available remedy regardless of breach, *e.g.*, for fraud where there has not otherwise been a breach.

In cases where the plaintiff's expectation damages will be too speculative to measure, the courts will look to a "reliance" measure of damages. Reliance damages measure costs incurred in reliance on the contract. They are designed to put the plaintiff in the position that would have pertained had the contract not been formed.<sup>345</sup>

---

<sup>342</sup> RESTATEMENT (SECOND) OF CONTRACTS § 378 (1981).

<sup>343</sup> A "unique" object of performance is a typical predicate to an inadequacy of remedy at law. *See, e.g.*, P.S. Atiyah, AN INTRODUCTION TO THE LAW OF CONTRACT 442-43 (4th ed. 1989).

<sup>344</sup> U.C.C. § 2-106(4); *cf.* U.C.C. § 2-720.

<sup>345</sup> *See* RESTATEMENT (SECOND) OF CONTRACTS § 349.



#### 4. Limitations on Remedies

A contract may provide for specific remedies or it may exclude claims for various types of damages.

##### a. Limitation on Consequential Damages

Given what amounts to a legal presumption against consequential damages, it should not be surprising that consequential damages may be validly excluded or limited by contract, provided the clause is not deemed unconscionable.<sup>346</sup> In commercial settings, there is generally a presumption that limitations on consequential damages are valid.<sup>347</sup> Nonetheless, one noted case held neither "bad faith nor procedural unconscionability" necessary to render a consequential damages limitation claim void. Rather, in a case involving a custom software package, that court determined that a clause which limited the contractual remedy

---

<sup>346</sup> The doctrine of unconscionability constitutes one of the few generally applicable blanket impediments to the enforceability of contracts or certain provisions thereof. Construing the Uniform Commercial Code's prohibition on unconscionability, U.C.C. § 2-302(1), one court noted, "Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party." *Williams v. Walker Thomas Furniture Co.*, 350 F.2d 445, 449 (D.C. Cir. 1965); *see also* 1 E.A. FARNSWORTH, FARNSWORTH ON CONTRACTS § 4.28, at 506 (1990). Importantly, the fact that a contract may be one of "adhesion" (offered on a take-it-or-leave-it basis) does not alone satisfy the "absence of meaningful choice" facet of the doctrine. An "element of surprise" is usually necessary. FARNSWORTH, *supra*, at 507-508. In the context of consumer goods, the U.C.C. provides that a "[l]imitation of consequential damages for injury to the person . . . is *prima facie* unconscionable but limitation of damages when the loss is commercial is not." U.C.C. § 2-720(3).

<sup>347</sup> *See, e.g.*, U.C.C. § 2-719(3); *Earman Oil Co., Inc. v. Burroughs Corp.*, 625 F.2d 1291, 1299 (5th Cir. 1980); *Office Supply Co., Inc. v. Basi/Four Corp.*, 538 F. Supp. 776, 788 (E.D. Wis. 1982); *U.S. Fibres, Inc. v. Proctor & Schwartz, Inc.*, 509 F.2d 1043 (6th Cir. 1975) (unconscionability rarely exists in commercial setting where parties are of equal bargaining power).



to the cost of repairs in the event of a "total and fundamental" breach on the part of the vendor was unenforceable.<sup>348</sup>

## **b. Liquidated Damages**

In order to limit liability and to reduce the time, risk and expense of litigation on the issue of the measurement of damages, contracts often contain "liquidated damages" clauses, which are designed to establish the parties' liability in advance on the basis of a fixed sum or simple formula, such as a refund of the amounts paid under the contract over a certain period in time.<sup>349</sup> In general, such advance measurements are enforceable provided they do not constitute "penalties" and that (1) the actual damages will be uncertain in amount or difficult to prove, (2) the parties so intend to liquidate them in advance, and (3) the liquidated amount is not greatly disproportionate in amount to the "presumable" loss or injury.<sup>350</sup>

It is suggested that liquidated damages provisions will be unworkable in the FCA context unless consequential damages are validly excluded as a matter of law or by contract. Given the potentially limitless number, type and value of communications<sup>351</sup> to which certified digital signatures may be attached, attempting to liquidate consequential damages at the outset would be futile.

---

<sup>348</sup> *RRX Indus. Lab-Con, Inc.*, 772 F.2d 543 (9th Cir. 1985); *see also* *Hawaiian Tel. Co. v. Microfilm Data Sys., Inc.*, 829 F.2d 919 (9th Cir. 1987). In France, there is a growing reluctance to enforce clauses granting exemptions from liability. Citing the "essential obligations of the debtor, contractual good faith, or law and order," legal practice considers that certain obligations such as the provision of security form a totally integral part of the contract in certain cases that cannot be waived by contract. *See* G. Viney, *Les conventions d'irresponsabilité - droit français*, reprinted in *Recueil in Memoriam Jean Limpens* (Kluwer, Antwerp, 1987).

<sup>349</sup> Examples include the damages provisions in certain "Value-Added Network" contracts, which are discussed in Section VIII.B., *infra*.

<sup>350</sup> *See* *Shapiro v. Grinspoon*, 27 Mass. App. Ct. 596 (1989); *Banta v. Stamford Motor Co.*, 92 A. 665, 667 (Conn. 1914). The Uniform Commercial Code has relaxed this standard to a degree by requiring only that, in the context of contracts for the sale of goods, the liquidated amount be "reasonable in the light of the anticipated or actual harm caused by the breach, the difficulties of proof of loss, and the inconvenience or nonfeasibility of otherwise obtaining an adequate remedy." U.C.C. § 2-718(1).

<sup>351</sup> Restrictions can be imposed on the type and value of such communications by implementing, *e.g.*, authentication certificates.

### c. Punitive Damages

Punitive damages are generally not recoverable for breach of contract, although jurisdictions differ on the question. In general, punitive damages are only available in situations where the breach is also a tort that by itself would give rise to punitive damages: "Where the conduct alleged breaches a legal duty which exists independent of the contractual relations between the parties, a plaintiff may sue in tort because the plaintiff may recover in tort whether or not he has a valid claim for breach of contract."<sup>352</sup>

Punitive damages are also allowed if so provided in the contract or when the defendant engaged in, for example, negligent or intentional misrepresentations or fraud.<sup>353</sup> In a case where a car was repossessed on the basis of faulty computer records, even after the plaintiff provided notice of payment on at least three occasions, punitive damages were allowed, in part, due to defendant's improper reliance on computer-based records.<sup>354</sup>

### E. GENERAL TORT LIABILITY CONSIDERATIONS (INCLUDING DAMAGES)

Unlike contract, tort law has generally grown into a series of more or less discrete causes of action that have peculiar applicability to different fact situations. This section discusses a number of torts related specifically to information and information technology that are likely to be relevant to future judicial analysis of FCA activities. "Broadly speaking, a tort is a civil wrong, other than breach of contract, for which the court will provide a remedy, in the form of an action for damages."<sup>355</sup> The function of tort "is directed toward the compensation of individuals, rather than the public, for losses which they have suffered within the scope of their legally recognized interests generally, rather than one interest only,

---

<sup>352</sup> *Hargrave v. Oki Nursery, Inc.*, 636 F.2d 897, 899 (2d. Cir. 1980).

<sup>353</sup> See *Glovatorium v. NCR Corp.*, 684 F.2d 658 (9th Cir. 1982) (awarding punitive damages of more than \$2,000,000 nearly 10 times actual damages awarded).

<sup>354</sup> See *Ford Motor Credit Co. v. Swarens*, 447 S.W.2d 553 (Ky. 1969); see also *Price v. Ford Motor Credit Co.*, 530 S.W.2d 249 (Mo. App. 1975); *Ford Motor Credit Co. v. Hitchcock*, 158 S.E.2d 468, 470-73 (Ga. App. 1967).

<sup>355</sup> PROSSER, *supra* note 197, § 1.



where the law considers that compensation is required."<sup>356</sup> "As a general principal, liability in tort must be based upon conduct which is socially unreasonable. The common thread woven into all torts is the idea of unreasonable interference with the interests of others."<sup>357</sup> It is generally agreed that tort liability can be imposed for any of three reasons:

1. Intent of the defendant to interfere with the plaintiff's interests.
2. Negligence.
3. Strict liability, "without fault," where the defendant is held liable in the absence of both intent to interfere with the plaintiff's interests and negligence.<sup>358</sup>

This section should be read with the understanding that there is a history of inventing new torts to respond to the needs of society. Perhaps the relative novelty of the FCA's activities will prompt the development of new torts.

### 1. Liability for Defective Information Technology (Negligence)

The extent of the FCA's liability if it were to sell defective information technology would depend on the liability regime under which the FCA is evaluated. The two major alternatives are regimes of negligence and strict liability. The occurrence of an error *per se* would not generally suffice to create liability: errors are to be expected in information systems. And when a supplier of information is dealing with large numbers of users and volumes of information, the likelihood of errors increases. Users should not expect a fail-safe system, but should be entitled to expect the vendor to adopt procedures calculated to establish a reasonable level of reliability.

---

<sup>356</sup> *Id.* at 5-6. "Perhaps more than any other branch of the law, the law of torts is a battleground of social theory. Its primary purpose, of course, is to make a fair adjustment of the conflicting claims of the litigating parties. But the twentieth century has brought an increasing realization of the fact that the interests of society in general may be involved in disputes in which the parties are private litigants." *Id.* § 3, at 15.

<sup>357</sup> *Id.* § 1 (Supp. 1988) (citing *Smith v. Superior Court*, 198 Cal. Rptr. 829 (1984)).

<sup>358</sup> *Id.* § 7.

## Duty of Care and Measure of Damage

Generally, there is a duty to exercise reasonable care with respect to the design, manufacture and operation of information technology.<sup>359</sup> Thus, when a security company failed to include features in its software program that would contact the police in the event of a burglary, the company was found to have breached a duty to exercise reasonable care.<sup>360</sup> Also, a telephone company has been found liable for the negligent loss of computer data.<sup>361</sup>

Additionally, the FCA would not necessarily be able to defend itself on the basis that it was following generally accepted security standards for the computer industry:

Indeed in most cases reasonable prudence is in fact common prudence, but strictly it is never its measure; a whole [industry] may have unduly lagged in the adoption of new and available devices. [The industry] may never set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal regard will not excuse their omission . . . .<sup>362</sup>

Thus, a trucking company that failed to use available computing equipment to monitor driver fatigue has been considered negligent.<sup>363</sup>

Damages under a negligence regime may well exceed the consequential damages possible in contract discussed previously in connection with the *Evra* case:<sup>364</sup> damages are measured by the concept of proximate cause which is broader than mere foreseeability. Because the FCA may be the only entity offering services of this type, a defect or breakdown in FCA communications could result in significant damages either because no alternative service would be available to the user, or because the breakdown in which the defect is discovered would be

---

<sup>359</sup> See *Bradford Trust Co. v. Texas Am. Bank*, 790 F.2d 407 (5th Cir. 1986) (duty to minimize impact even of unexpected occurrences).

<sup>360</sup> See *Ostalkiewicz v. Guardian Alarm*, 520 A.2d 563 (R.I. 1987).

<sup>361</sup> See *Ed Fine Oldsmobile, Inc. v. Diamond State Tel. Co.*, 494 A.2d 636 (Del. 1985).

<sup>362</sup> *The T. J. Hooper*, 60 F.2d 737, 740 (2nd Cir.), *cert. denied*, 287 U.S. 662 (1932) (ship negligent for failure to have used available technology (weather radio)).

<sup>363</sup> *Torres v. North Am. Van Lines, Inc.*, 658 P.2d 835, 838-39 (Ariz. App. 1982).

<sup>364</sup> See Section VI.D.3., *supra*. In *Evra* itself, the court noted that conceptions of liability in tort and contract "link up." 673 F.2d at 958.



significant in itself. The FCA would generally have a duty to take steps to ensure reliability when the burden of those measures is less than the probability of a loss multiplied by its magnitude.<sup>365</sup> This could create a fairly high standard of care for the FCA because information defects are inevitable and potential loss could be great.

If the FCA is put on notice or has knowledge of the level of the User's dependence on certification technology, contractual limitations on consequential damages might be deemed unconscionable by a court.

The FCA could argue in response that the plaintiff had improperly relied upon certification technology. The cases recognize that, because errors can and will occur in information systems, users must exercise caution in delegating decisions to a computer system for handling in a standardized manner.<sup>366</sup> When a user knows or should have known the possibilities for error, it cannot ignore that knowledge (or imputed knowledge) and must take action to prevent harm. There are also limitations that may be placed on liability when the user has relied uncritically upon computer-generated information and has acted in a manner that precludes alternative methods of consummating a transaction. While the user's contributory negligence would prohibit any recovery in only a restricted number of cases of user misuse,<sup>367</sup> some sort of comparative negligence system is the typical practice.

## **2. Liability for Defective Information Technology (Strict Liability)**

The FCA might also be evaluated under that part of the evolving law of products liability which is grounded in strict liability. Strict liability is a term that means liability without fault.<sup>368</sup> To be held strictly liable, a plaintiff in a products liability action need only show that (i) the defendant manufactured or supplied a product which was defective when it left the defendant's control; (ii) that the plaintiff was injured by the product; and (iii) that the defective condition was the proximate cause of the plaintiff's injury.<sup>369</sup>

---

<sup>365</sup> See, e.g., *U.S. v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947), *reh'g denied*, 160 F.2d 482 (1947).

<sup>366</sup> See *Memphis Light, Gas & Water Div. v. Craft*, 436 U.S. 1 (1978); *Palmer v. Columbia Gas of Ohio, Inc.*, 479 F.2d 153 (6th Cir. 1973).

<sup>367</sup> See H. S. Koh, *Liability for lost or stolen funds*, 91 CORNELL INT'L L.J. 99 (1989).

<sup>368</sup> See PROSSER, *supra* note 197, § 13, at 534 *et seq.*

<sup>369</sup> *In re Asbestos Cases*, 847 F.2d 523, 525 n.2 (9th Cir. 1988).

If the FCA were treated as providing a *product* (e.g., a defective certificate) rather than a *service*,<sup>370</sup> and where the resulting injury is not wholly economic (i.e., personal injury results), then there is a basis for strict liability.<sup>371</sup> There is also a growing application of products liability law to products containing defective information. These cases have mainly been pursued where plaintiff's damages have been to person or property.<sup>372</sup> Often the focus of the cases has been on mass-produced information products.<sup>373</sup> Because there has historically been an ever-increasing scope of strict liability for damages,<sup>374</sup> the possibility that the FCA

---

<sup>370</sup> See Section VI.D.1., *supra* (concerning whether the FCA provides services or goods). In *Johnson v. Sears, Roebuck & Co.*, 355 F. Supp. 1065 (E.D. Wis. 1973), the court rejected the good vs. service distinction in human blood sales and held the provider strictly liable in tort. The judge wrote that his "decision would not be based on a technical or artificial distinction between sales and services. Rather, I must determine if the policies which support the imposition of strict liability would be furthered by its imposition in this case." *Id.* at 1066. See *Bryant v. Tri-County Electric Membership Corp.*, 844 F. Supp. 347 (Ky. 1994) (holding that electricity a "product" and is "sold"; electric utility is subject to strict product liability). *Bryant* noted that at least eight of the ten states that have considered this issue have concurred. *Id.* at 360 n.6.

The goods/services distinction appears to be disintegrating world-wide: "[I]n all cases where the information provided is supplied in a medium that gives it the appearance of a "product" - and this would apply to a ROM compact disc - automatic liability on the part of the producer should come into play, by virtue of an EC directive dated 25 July 1985 relating to strict liability for defective products." Huet, *Product Liability In The Information Field*, reprinted in *INTERNATIONAL CONTRACTS FOR SALE OF INFORMATION SERVICES* 157, 168 (1988).

<sup>371</sup> See *MacPherson v. Buick Motor Co.*, 111 N.E. 1050 (N.Y. 1916). Not all jurisdictions recognize strict liability, however.

<sup>372</sup> See Section VI.C.2.c., *supra* (concerning economic loss generally); see also *APLications Inc. v. Hewlett-Packard*, 672 F.2d 1076 (2d Cir. 1982).

<sup>373</sup> See, e.g., *Salomey v. Jeppesen & Co.*, 707 F.2d 671, 676-677 (2d Cir. 1983); *Aetna Casualty and Surety Co. v. Jeppesen & Co.*, 642 F.2d 339, 341-42 (9th Cir. 1981) (air navigation charts); *Brocklesby v. U.S.*, 767 F.2d 1288, 1294-95 (9th Cir. 1985), *cert. denied*, 474 U.S. 1101 (1986).

<sup>374</sup> Virtually all types of damages may be compensable without a showing of fault on the part of the vendor or manufacturer of the goods.



would be held strictly liable, even in the absence of personal injury, deserves mention.

Although there may be difficulty in proving that a certificate issued by the FCA was defective, in that proofs of the strength of and the absence of *trap doors* in cryptographic algorithms are not currently possible, the possibility remains that defects in FCA-designed or -provided hardware or software could create defective information or cause an information breakdown.

Most jurisdictions require that for a vendor to be held strictly liable the product must be *unreasonably dangerous* for its intended use.<sup>375</sup> In other jurisdictions, the vendor may be liable if its product does not meet its own specifications, for whatever reason, or if the properly constructed product contains design defects. The vendor may also be liable for failing to provide warnings regarding risks related to the intended (or unintended) use of the product<sup>376</sup> or regarding reasonably foreseeable dangers which may arise from its use.<sup>377</sup>

Another relevant standard for a design defect is whether the vendor has reduced the level of risk to the greatest degree possible, consistent with the product's utility. For example, the FCA could not be expected to establish such high safeguards that its certification system would become inefficient to use. Other factors include whether the user can be held responsible for incurring a reasonable assumption of risk, such as any user knowledgeable of a computer system's fallibilities might make, thus relieving the vendor of responsibility for certain risks. The manner in which the user used or misused the product would be relevant; a user's assumption of a specific risk in the face of known dangers will often constitute a bar to the recovery of damages.<sup>378</sup> With these complicating factors considered, products liability can take on certain of the *attribution of fault* aspects of the negligence system.

The manufacturer of faulty aviation charts has been found strictly liable for an air disaster.<sup>379</sup> Another case noted in dicta that computer software might be

---

<sup>375</sup> See RESTATEMENT (SECOND) OF TORTS § 402A.

<sup>376</sup> See, e.g., *Cronin v. J.B.E. Olsenn Corp.*, 8 Cal. 3d 121, 134 (1972).

<sup>377</sup> See *Midgley v. S.S. Kresge Co.*, 55 Cal. App. 3d 67, 71 (1976).

<sup>378</sup> See *Findley v. Copeland Lumber Co.*, 509 P.2d 28 (Or. 1973); RESTATEMENT (SECOND) OF TORTS § 402A.

<sup>379</sup> See *Aetna Casualty and Surety Co. v. Jeppesen & Co.*, 642 F.2d 339 (9th Cir. 1981); see also RESTATEMENT (SECOND) OF TORTS § 402A cmts. (c), (f) (1965).

considered a "product" for product liability purposes.<sup>380</sup> No reported cases have been found in which the courts have held the vendor of software strictly liable under products liability standards.<sup>381</sup> However, the FCA should be aware that such liability may in the future expand to include software and information service providers. On the other hand, because the FCA will provide what might easily be termed *experimental products*, it might thereby earn a degree of liability protection.<sup>382</sup> With an experimental product, fewer assurances might reasonably be expected, and users might consequently have to assume a greater degree of risk. The same sort of analysis may also apply to the FCA's ability to give assurances concerning the content of the information it handles.

Finally, strict liability for information products should be examined for its possible chilling effect on free speech. One threshold issue in this area would be whether a CA's information products (e.g., certificates) would more closely resemble more closely a mass-produced good, such as a credit card, or a more particularized expression, such as a book. If the certificate were considered to resemble a mass-produced good, it would receive a lower degree, if any, of protection.<sup>383</sup>

---

<sup>380</sup> See *Winter v. G. P. Putnams's Sons*, 938 F.2d 1033 (9th Cir. 1991).

<sup>381</sup> Cf. *Antel Oldsmobile-Cadillac, Inc. v. Sirius Leasing Co.*, 475 N.Y.S.2d 944, 945 (1984) (refusing to hold defendant strictly liable for defect that caused loss of data).

<sup>382</sup> See, e.g., *Winter Panel Corp. v. Reichhold Chems., Inc.*, 823 F. Supp. 963 (D. Mass. 1993) (consequential damage limitation clause in invoice not unconscionable where both parties were commercial entities and product was experimental). "Particularly here, where the product at issue was a complex, sophisticated, and at the time experimental substance, it was permissible and appropriate for commercial entities to allocate the risks of potential failure." *Id.* at 973; see also *Logan Equip. Corp. v. Simon Aerials, Inc.*, 736 F. Supp. 1188 (D. Mass. 1990).

<sup>383</sup> Cf. *Brocklesby v. U.S.*, 767 F.2d 1288 (9th Cir. 1983) (detailed navigational charts not characterized as protected speech). But see, *contra*, *Jones v. J.B. Lippincott Co.*, 694 F. Supp. 1216, 1217 (D. Md. 1988); *Daniel v. Dow Jones & Co. Inc.*, 520 N.Y.S.2d 334, 339-40 (1987) (determining that computerized on-line services were protected speech); *Dun and Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 755-63 (1985). Commercial speech need not be regulated by the *least restrictive* means, but instead by *reasonable* means. See *Board of Trustees v. Fox*, 493 U.S. 887 (1989).



### 3. European Directives and Products and Services Liability

The Council of the European Communities has issued a "Council Directive Concerning Liability for Defective Products" dealing exclusively with moveable products,<sup>384</sup> which assigns liability based on whether the vendor met the user's reasonable expectations of the vendor's safety standards. A draft proposal for services utilizes the same standard.<sup>385</sup> In the Directive Draft, fault is presumed except when the vendor can establish that it used reasonable security measures. With such a burden, the injured person must only provide proof of the damage and the causal link between the provision of services and that damage. The directive is intended to provide better protection to consumers who receive services on a private basis.

The Directive Draft also covers damages directly caused by service businesses to the health or physical integrity of persons or their private property. Again, the burden of proof in establishing absence of fault is on the supplier. The Directive excludes "public services intended to maintain the public safety as well as damage covered by international liability agreements ratified by Member States or the Community."

Only services provided by a commercial trader would be covered. Force majeure or compliance with legally binding rules can remove liability. A three year limitation period would run from the date the victim became aware of the safety defect until the victim identified the supplier of services. The postal and transport services have asked to be excluded from this proposal. Yet to be settled is impact of the provision of insurance services.<sup>386</sup>

---

<sup>384</sup> Doc't No. 85/374/EEC (July 25, 1985), O.J. No. L 210, at 29. The directive came into force on July 30, 1988.

<sup>385</sup> EUR. COMM'N, DRAFT PROPOSAL FOR A COUNCIL DIRECTIVE ON THE LIABILITY OF SUPPLIERS OF SERVICES, COM(90) 482 final - SYN 308 (91/C 12/11) (Nov. 9, 1990) [hereinafter DIRECTIVE DRAFT]. Cf. AMENDED PROPOSAL FOR A DIRECTIVE ON THE PROTECTION OF CONSUMERS IN RESPECT OF CONTRACTS NEGOTIATED AT A DISTANCE (DISTANCE SELLING), O.J. No. C158/14 (1992) (considers consumer computer-based commerce).

<sup>386</sup> See generally Section IX.B., *infra* (concerning insurance).

#### 4. Negligently Undertaking to Provide Security

This action in tort generally applies only in cases of physical harm. It is relevant because it involves an agreed-upon or voluntarily provided security regime and new areas of computer law are likely to be analyzed by analogy to existing legal standards. A hospital and security firm, for example, were found negligent in failing to adequately warn or protect the plaintiff, thereby contributing to a violent criminal assault:<sup>387</sup>

A landlord may, as indicated, incur a duty voluntarily or by specific agreement if to attract or keep tenants he provides a program of security. A program of security is not the usual and normal precautions that a reasonable home owner would employ to protect his property. It is, as in the case before us, an extra precaution, such as personnel specifically charged to patrol and protect the premises. Personnel charged with such protection may be expected to perform their duties with the usual reasonable care required under standard tort law for ordinary negligence. When a landlord by agreement or voluntarily offers a program to protect the premises, he must perform the task in a reasonable manner and where a harm follows a reasonable expectation of that harm, he is liable. The duty is one of reasonable care under the circumstances. It is not the duty of an insurer and a landlord is not liable unless his failure is the proximate cause of the harm.<sup>388</sup>

A danger to tenants is considered foreseeable, for example, where the premises are in a high crime area, security is lax, outsiders have access to the premises and there have been prior instances of crime on the premises.<sup>389</sup> Courts have found a duty to protect customers from armed robberies, at least by taking minimal deterrent security precautions.<sup>390</sup> A similar analysis could be applied in computer security cases.

#### 5. Professional Negligence/Computer Malpractice

Professional negligence constitutes a failure to act reasonably in light of the special knowledge, skills and ability which a member of a particular profession is expected to possess. The reasonable act of an ordinary person may become unreasonable in light of special knowledge, skills and ability.<sup>391</sup>

---

<sup>387</sup> See *Kerns v. Methodist Hosp.*, 1990 WL 55974 (Pa. 1990); cf. *Glick v. Olde Towne Lancaster*, 535 A.2d 621 (Pa. Super. 1987).

<sup>388</sup> *Id.* (citing *Feld v. Merriam*, 485 A.2d 742 (Pa. 1985)).

<sup>389</sup> See *Kwaitkowski v. Superior Trading Co.*, 123 Cal. App. 3d 324 (1981).

<sup>390</sup> See *Cohen v. Southland Corp.*, 157 Cal. App. 3d 130, 138 n.1 (1984).

<sup>391</sup> *Data Processing Servs., Inc. v. L.H. Smith Oil Corp.*, 492 N.E.2d 314 (Ind. App. 1986) (computer programming).



Liability under this theory rests on a three-fold analysis. First, it must be established that the function provided by the professional requires special knowledge, skills, or ability. Second, the professional must know or have reason to know that users are relying upon that knowledge and ability. Third, it must be reasonable for the professional to have foreseen that the user would suffer a loss if the professional did not perform with requisite skill and ability.<sup>392</sup>

The courts have generally frowned upon the establishment of a malpractice cause of action in the computer programming field. The crux of a malpractice claim is that the tort occurred within the context of the delivery of professional services. Computer programming, however, lacks the attributes commonly associated with professional status. Programmers are not restricted by state regulations or licensing, they do not regulate themselves, and they are not required to complete a specified course of education or training. Consequently, the cases bearing on the malpractice issue have generally rejected the idea of programmers as professionals.<sup>393</sup>

---

<sup>392</sup> See *id.*

<sup>393</sup> Zammit, *Tort Liability for Mishandling Data*, 13th Annual Computer Law Institute 429-34 (Prac. Law. Inst. 1991) (citing *Hospital Computer Systems*, 788 F. Supp. 1351 (D.N.J. 1992) (computer consultants); *RKB Enterprises*, No. 64614 (N.Y. App. Div. Feb. 6, 1992) (computer consultant); *Chaltos Systems, Inc. v. National Cash Register Corp.*, 479 F. Supp. 738 (D.N.J. 1979), *aff'd in part*, 635 F.2d 1081 (3d Cir. 1980), *cert. denied*, 457 U.S. 1112 (1982); *Triangle Underwriters, Inc. v. Honeywell, Inc.*, 457 F. Supp. 765, 770-71 (E.D.N.Y. 1978). Other courts have applied an "ordinary care" standard for computer professionals as well. See, e.g., *Invacare Corp. v. Sperry Corp.*, 612 F. Supp. 488 (N.D. Ohio 1984).

In the context of licensing programmers to mitigate risks, Peter G. Neumann, SRI, widely known for his moderation of the Internet RISKS-Forum has stated,

I'm ambivalent. Its one of these double-edged swords. The licensing process is often lowest-common-denominator stuff. In order to get the certification process through, you end up with the minimum set of skills that people need to have. And yet, if they are dealing with life-critical systems, they need to have a tremendous amount of experience, creativity, imagination, a sense of what won't work and a conservative attitude towards development. There is no way you can establish certification procedures that will ferret out those traits. My bottom line is that certification procedures would be wonderful if they could be made to work, but I don't think that they can be made to work -- especially for critical systems.

S. Garfinkel, *The Dean of Disaster*, WIRED, Dec. 1993, at 46 (quoting P. Neumann).

Nonetheless, other courts have imposed a higher standard of care.<sup>394</sup> It is unclear whether FCA personnel should or will be held to a professional standard of care.<sup>395</sup> Also, in the immediate future, when CA operations will necessarily be somewhat experimental, it would seem premature to *professionalize* operation and management of CAs before performance standards have a chance to be developed, tested and agreed upon.

## 6. Gross Negligence

Gross negligence is defined as "a failure to exercise even that care which a careless person would use . . . [and several courts include a requirement of] willful, wanton or reckless misconduct, or such utter lack of all care as will be evidence thereof."<sup>396</sup> Gross negligence may diminish or eliminate the enforceability of limitations of damages clauses in contracts.

## 7. Punitive Damages

"[E]xcessive reliance on computer data without proper safeguards to ensure the reliability and accuracy of the information may constitute the failure to exercise due care, and in some cases may even result in the award of punitive damages."<sup>397</sup>

## F. SUBSIDIARY (CIVIL) LIABILITY ISSUES

### 1. Anti-Competitive Considerations

The basic principles of federal antitrust law are contained in the Sherman Act of 1890.<sup>398</sup> Section 1 of the Sherman Act prohibits "[e]very contract, combination in

---

<sup>394</sup> See, e.g., *Diversified Graphics v. Groves* 868 F.2d 293 (8th Cir. 1989) (holding Ernst & Whinney to higher standard concerning computer expertise); *L.H. Smith Oil Corp.*, 492 N.E.2d 314.

<sup>395</sup> See generally Section IX.A.2., *infra* (concerning accreditation of professionals).

<sup>396</sup> PROSSER, *supra* note 197, § 34, at 212.

<sup>397</sup> U.S. DEP'T OF JUSTICE, COMPUTER CRIME COMPUTER SECURITY TECHNIQUES (1980).

<sup>398</sup> Ch. 647, 26 STAT. 209 (July 2, 1890) (codified at 15 U.S.C. §§ 1-7).



the form of trust or otherwise, or conspiracy, in restraint of trade or commerce."<sup>399</sup> Section 2 declares that "[e]very person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of . . . trade or commerce . . . shall be deemed guilty of a felony . . . ." <sup>400</sup> Thus, the Sherman Act takes aim at two forms of anti-competitive behavior: "collusive" practices and "exclusionary" practices."<sup>401</sup> Other provisions of antitrust law, including the Clayton Act,<sup>402</sup> the Federal Trade Commission Act,<sup>403</sup> and the Robinson-Patman Antidiscrimination Act,<sup>404</sup> can be viewed as more specific implementations of these principles.

The applicability of antitrust law to the FCA is extremely problematic, on several levels. First, "collusive" practices require more than one enterprise engaged in the provision of the same or similar goods or services. Because the scope of the FCA's activities and the market structure in which it will operate are undetermined, not even the base potential for difficulties on this front can be assessed at this time. The establishment of a "monopolistic" FCA raises a more coherent threat of

---

<sup>399</sup> 15 U.S.C. § 1. See *Continental Airlines v. American Airlines*, 1993 WL 379396 (S.D.Tex.).

<sup>400</sup> 15 U.S.C. § 2.

<sup>401</sup> R. POSNER, *ANTITRUST LAW: AN ECONOMIC PERSPECTIVE* 28 (1976).

<sup>402</sup> Ch. 323, 38 STAT. 731 (Oct. 15, 1914). In general, the Clayton Act as amended prohibits "tie-ins" (15 U.S.C. § 14) and certain acquisitions of stock or assets, "the effect of [which] acquisitions may be substantially to lessen competition, or to tend to create a monopoly. . . ." (15 U.S.C. § 18).

<sup>403</sup> 38 STAT. 719 (Sept. 26, 1914). "Unfair methods of competition in or affecting commerce, and unfair deceptive acts or practices in or affecting commerce, are declared unlawful." 15 U.S.C. § 45(a). This statute has been "held to forbid virtually anything forbidden by any other antitrust provision, and then some." POSNER, *supra* note 401, at 30 (citing *FTC v. Brown Shoe Co.*, 384 U.S. 316 (1966)).

<sup>404</sup> Ch. 592, 49 STAT. 1526 (June 19, 1936). Robinson-Patman explicitly forbids discrimination in the price of commodities "where the effect of such discrimination may be substantially to lessen competition or tend to create a monopoly in any line of commerce, or to injure, destroy, or prevent competition with any person . . . " and the sale of goods "at unreasonably low prices for the purpose of destroying competition or eliminating a competitor." 15 U.S.C. §§ 13, 13a.

liability for "exclusionary" practices such as "tie-in" arrangements,<sup>405</sup> predatory pricing,<sup>406</sup> vertical integration and exclusive dealing practices,<sup>407</sup> and boycotting.<sup>408</sup> All or most of these problems could be abolished at a stroke with appropriate legislation or administrative action, or by necessary implication of a federal contract for FCA services. Finally, although regulation as a common carrier includes certain exemptions from the provisions of antitrust law,<sup>409</sup> the AT&T case provides ample evidence of the important implications for common carriers of antitrust law.<sup>410</sup> It is perhaps fortunate both that the Federal Trade Commission and NIST reside within the Department of Commerce. The consequent convergence of administrative authority can facilitate proper planning and guidance so as to avoid antitrust difficulties to the greatest possible extent before they arise.

---

<sup>405</sup> "Tie-in" arrangements are those by which the seller of one product seeks to extend monopoly power into other markets by requiring buyers of the first product to purchase another. *See* POSNER, *supra* note 401, at 171-72. A rather crude example of this conduct in the FCA context might be a requirement that certificate holders utilize FCA facilities for all of their electronic messaging needs, including those not involving digital signatures.

<sup>406</sup> *See* Posner, *supra* note 401, at 184. It is not inconceivable, for example, that the FCA might seek to drive VANs out of business by using certificate generation and/or maintenance revenues, which would theoretically be necessary to cover potential liabilities for certification to subsidize unlawful "pricing" wars in the network communications market. The difficulties of proving monopolistic "intent" were recently demonstrated in *Continental Airlines, Inc. v. American Airlines and AMR Corp.*, 1993 WL 379396 (S.D. Tex.), 1993-2 Trade Cas. (CCH) ¶ 70,334.

<sup>407</sup> *See* POSNER, *supra* note 401, at 196-207. The acquisition of, or the execution of exclusive dealing contracts from VANS or notarial bodies might give rise to liability under these headings.

<sup>408</sup> *See* POSNER, *supra* note 401, at 207-211.

<sup>409</sup> *See, e.g.*, 15 U.S.C. § 18 ("Nothing contained in this section shall apply to transactions duly consummated pursuant to authority given by the . . . Federal Trade Commission. . . .").

<sup>410</sup> *See* *U.S. v. AT&T Co.*, 552 F. Supp. 131 (D.D.C. 1982) (subsequent history omitted); *see also*, 47 U.S.C. § 313(a) (radio communications activities subject to antitrust laws).



## 2. Defamation

A definition of a defamatory communication is "one which tends to hold the plaintiff up to hatred, contempt or ridicule, or to cause him to be shunned or avoided [or more appropriately] that which tends to injure 'reputation' in the popular sense; to diminish the esteem, respect, goodwill or confidence in which the plaintiff is held."<sup>411</sup> Whether the FCA, as the maintainer of a data base and facilitator of communications, will be considered a *publisher* or merely a *distributor* of defamatory statements will affect its liability. The FCA would be shielded from liability to a considerable degree if it were deemed a distributor only.<sup>412</sup> Although the use of cryptographic technology could operate as a practical bar to the exercise of editorial supervision, "publisher" status might arise if certificates (particularly attribute certificates) or CRLs containing defamatory information were viewed as a result of the FCA exercising editorial control over the information, which might be necessary in naming, granting, or limiting authority, and in establishing cause for placing a certificate on a CRL.

To illustrate, when a Social Security Administration's data entry error resulted in an investigation for fraud on the basis of poor credit, the plaintiff recovered on a negligence claim notwithstanding exculpation by a lower court under the Federal Tort Claims Act. The court noted that the Social Security Administration had a duty to implement verification and audit procedures.<sup>413</sup>

The related tort of "injurious falsehood or disparagement" has been defined as, "the publication of matter derogatory to the plaintiff's title to his property, or its quality, or to his business in general, or even to some element of his personal affairs, of a kind calculated to prevent others from dealing with him, or otherwise to interfere with his relations with others to his disadvantage."<sup>414</sup> Pecuniary loss, communication to a third party and falsehood must be proven.

A CRL is intended precisely to "prevent others from dealing with" the subject of the CRL. However, the standard for this tort is steep. The plaintiff must prove

---

<sup>411</sup> PROSSER, *supra* note 197, § 111 at 773.

<sup>412</sup> See, e.g., *Cubby, Inc. v. Compuserve Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) (finding provider of computer-based data base to be a distributor where there was no evidence that it knew or had reason to know of defamatory statements). See also ELECTRONIC CONTRACTING, *supra* note 2, § 9.53, at 974-75.

<sup>413</sup> See *Jiminez-Nieves v. U.S.*, 682 F.2d 1 (1st Cir. 1982), on remand, 618 F. Supp. 66 (D. P.R. 1985).

<sup>414</sup> PROSSER, *supra* note 197, § 128, at 967.

that the communication was false and malicious, that it was communicated to a third party, and that pecuniary loss occurred as a result. Moreover, absolute privilege will likely protect the FCA even where there is malice. The rules and common law surrounding companies that track and report credit rating would be relevant here. Credit reporting companies show that it is certainly possible to provide information that may limit another party's business without necessarily being found liable in tort. One problem the CA might face is that security may be harder to define objectively than for example, a credit rating. Also, aspects of the negligent or wrongful dishonor of a check should be reviewed.<sup>415</sup>

---

<sup>415</sup> See U.C.C. §§ 3-502 (Dishonor), 3-503 (Notice of Dishonor), 3-504 (Excused Presentment and Notice of Dishonor) 3-505 (Evidence of Dishonor).



### 3. Interference with Contractual Relations; Franchising

#### Contractual Relations

"[I]n many cases interference with contract is not so much a theory of liability in itself as it is an element of damage resulting from the commission of some other tort, or the breach of some other contract."<sup>416</sup> The FCA could be liable for such interference, for example, by restricting, delaying or denying issuance of certificates. Also, a CRL could be seen as a "drop dead" device. In cases that have dealt with "drop dead" or disabling devices, software providers used an imbedded (and typically undisclosed) mechanism to shut down the subject application(s), usually activated in the event of a dispute, resulting in vendor liability. The requirements and procedures for CRL generation should be considered in light of these decisions.<sup>417</sup> The inappropriate generation of a CRL might potentially be considered an actionable interference with contractual relationships.

#### Franchising

Although most relevant in commercial contexts, certain franchise laws and regulations may present additional potential risks to CAs. A franchise relationship is characterized

by the payment of a fee for the right to distribute goods or services substantially associated with a trademark or other commercial symbol of the grantor under a marketing plan or system prescribed in substantial part by the grantor or in which the grantor and grantee have a community of interest in marketing the product.<sup>417A</sup>

---

<sup>416</sup> PROSSER, *supra* note 197, § 129, at 992.

<sup>417</sup> See, e.g., *Revlon Inc. v. Logisticon Inc.*, Comp. Indus. Litig. Rep., 12156, 12176, 12512 (1990); *Frank & Sons v. Information Solutions Inc.*, 8 C.L.S.R. 868 (N.D. Okla. 1988), noted in Comp. Indus. Litig. Rep., 8927-35 (Jan. 23, 1989); *Art Stone Theatrical Corp. v. Technical Programming and Sys. Support*, 549 N.Y.S.2d 789 (1990) (wrongful removal of source code); *Burleson v. State*, 802 S.W.2d 429 (Tex. Ct. App. 1991) (logic bomb in employer's application program).

<sup>417A</sup> W. Scott, "Business Labels, Identifying the signs of a franchise relationship," A.B.A. J. (Dec. 1993) at 86.

<sup>417B</sup> Disclosure Requirements and Prohibitions Concerning Franchising and Business Opportunity Ventures, 16 C.F.R. pt. 436. This regulation was enacted in 1979. See *Flynn v. Yogurt*, 1993 WL 454355 (D. Md) (concerning the Disclosure Rule's "direct marketing" requirement). See generally SCOTT, FRANCHISING LAW PRACTICE AND FORMS (1992).

A franchise relationship might be viewed as arising where subordinate certifiers (such as PCAs) pay a fee for the right to create and distribute certificates (*e.g.*, within a community of interest). Franchise laws requiring governmental registration of disclosure documents present an interesting analogy to possible requirements for PCA Policy Statement and agreement registration and approval. A breach of an implied covenant of good faith and fair dealing could violate the franchise laws in one or more of the approximately 18 states with such laws or the Federal Trade Commission's "Franchise Disclosure Rule,"<sup>417B</sup> which contains both civil and criminal penalties.

#### 4. Invasion of Privacy

In the civil sphere, the concept of invasion of privacy has emerged as four distinct torts: intrusion upon seclusion; appropriation of name or likeness; disclosure of private facts; and "false light" publicity.<sup>418</sup> As with the case of defamation, from which "false light" publicity is "virtually indistinguishable,"<sup>419</sup> the use of cryptographic methods presents a practical ban to unreasonable intrusion on, and publication of, private facts contained in encrypted transactions. However, information (*e.g.*, CRD) submitted to a CA could be the subject of an invasion of privacy.

On the other hand, the binding between a person and his certificate raises serious implications in terms of the "appropriation" branch of privacy tort law. One can imagine few more effective and complete appropriations of identity than to obtain and use another's certificate and/or private key in a commercial environment in which exclusive reliance is placed on the validity of certificates. Damages for appropriation would presumably consist of economic ones.<sup>420</sup>

---

<sup>418</sup> ELECTRONIC CONTRACTING, *supra* note 2, § 9.28, at 538.

<sup>419</sup> *Id.*

<sup>420</sup> *See id.* § 9.41, at 552.



Important other protections of privacy interests are provided by the United States Constitution,<sup>421</sup> the Privacy Act,<sup>422</sup> and the private rights of action provided under the Electronic Communications Privacy Act of 1986.<sup>423</sup>

---

<sup>421</sup> See Section VII.A.1., *infra*.

<sup>422</sup> 5 U.S.C. § 552a, discussed at Section VII.A.3.d., *infra*.

<sup>423</sup> 18 U.S.C. §§ 2520, 2707. The Electronic Communications Privacy Act is discussed at Section VI.G., *infra*.

## G. Criminal Liability

Until this point in this Report, FCA liability has been considered primarily as a civil matter. Criminal liability warrants attention as well, for two reasons. First, as a policy matter, the FCA's ability to deter and punish end-user recipient, FCA employee, and third party criminal conduct requires that the law sufficiently cover and protect unauthorized interference with FCA activities. Second, the uncertain status of FCA-related information in respect of other legal bases for the protection of information (such as copyright, patent and privacy)<sup>424</sup> may mandate specific criminal law implementations as an important avenue of protection.<sup>425</sup>

---

<sup>424</sup> Nimmer & Krauthaus, *supra* note 98, at 27 (criminal law protections advocated in the context of database information).

Commentators have noted that:

. . . the 'enforcement' approach [to deterrence] is [increasingly] under stress. There are too many violators, too many laws to be enforced, and not enough resources to get the job done. . . . [Consequently] information and analytic support will have to be provided for problems that have never been identified before, that may not look like typical police business, that might not have any relevant data readily available and that could turn out to be unique. Obviously, provision of the appropriate information support will require unprecedented creativity, improvisation, and innovation.

JFK School of Government, *Emerging Enforcement Strategies*, The Taubman Center Annual Report, 1992-1993, at 17 (1993).

<sup>425</sup> FCA-relevant activities that need to be methodically grounded in existing criminal laws or, that may require criminalization, have been proposed by one bank security analyst to include:

### Users:

False statement in CRD; Fraudulent Act committed using an FCA issued card/certificate; Theft or misuse of smart card; Intentional disclosure of private key; and Intentional unauthorized encrypting of company data by employee

### CA:

Tampering or theft of data and security modules; Wrongful disclosure of customer data; False statements in application for employment or professional certification; Theft or misuse of CA key; Intentional failure to make, or tampering with, CA journal entries; Tampering with trusted time clock or issuing falsely dated transactions; Failure to report breaches, frauds, crimes or data that came to light; and Working while intoxicated or otherwise impaired



## 1. Computer-Related Crime Generally

A "crime" has been defined as

an offense against the public at large, for which the state, as the representative of the public, will bring proceedings in the form of a criminal prosecution. . . . The civil action for a tort, on the other hand, is commenced and maintained by the injured person, and its primary purpose is to compensate for the damage suffered, at the expense of the wrongdoer. The state never can sue in tort in its political or governmental capacity, although as the owner of property it may resort to the same tort actions as any individual proprietor to recover for injuries to the property, or to recover the property itself.<sup>426</sup>

Liability for computer-based criminal acts is a developing area of the law and the extent and adequacy of current law accordingly remains uncertain. Statutory definitions of computer-related criminal acts are of course subject to controversial interpretation:

There is no single definition of [computer-related crime]. I may use the OECD [Organization for Economic Co-operation and Development] definition "computer abuse" to consider as "any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data" or a senior expert's definition "any illegal action in which a computer is a tool or object of the crime." What is more important is to understand that the computer today offers some highly sophisticated opportunities for law-breaking.

---

### Vendors:

Sale or inducement to use hardware/software containing a known trap door;  
and Failure to report security flaws promptly upon discovery

### Third Parties:

Hacking (as considered below); and Substituting an incorrect TLCA private key into a verifier's device

Memo from F. Sudia, Bankers Trust (Nov. 16, 1993).

Other basis of criminal liability related to software privacy should also be considered. See generally Software Publishers Ass'n, *Software Privacy, A Manual For Criminal Investigation and Prosecution* (1993) (providing a comprehensive treatment of software pirating, including: unauthorized copying, unauthorized distribution, software counterfeiting, hard disk loading, and BBS distribution).

<sup>426</sup> PROSSER, *supra* note 197, § 2, at 7.

A recent Council of Europe report distinguishes twelve different computer related illegal acts: computer related fraud; computer forgery; damage to computer data or programs; computer sabotage; unauthorized access; unauthorized interception; unauthorized reproduction of a protected computer program; unauthorized reproduction of a topography; alteration of computer data or computer programs; computer espionage; unauthorized use of a computer; unauthorized use of a protected computer program.

As there is a known difficulty with reporting such illegal acts to the police and going to court, estimates of losses suffered differ widely. There is no doubt, however, that we are talking of a problem with serious economic, social and strategic dimensions.<sup>427</sup>

Some of the critical issues that require careful review in connection with FCA-related computer-based criminal prosecution include the following:

- Whether anticipated FCA activities are sufficiently covered by existing criminal law or whether those activities require remedial legislative treatment and/or special remedial procedures particular to the FCA.
- Whether criminal statutes based upon illegal *access* adequately provide the basis for prosecution of improper FCA activities<sup>428</sup> or, instead, whether statutes are needed that address *unauthorized use* specifically.<sup>429</sup>

---

<sup>427</sup> G. Papapavlow, Head of Sector, *Legal aspects of new information technologies*, DG XIII-E1, Contribution to the Workshop on Electronic Signatures 1 (Brussels, Dec. 1, 1992). The difficulty in assessing the extent of the problem was noted by Don Parker of Stanford Research Institute: "There are no valid numbers representative of the size of the computer crime problem . . . [the published numbers] are false and meaningless." R. Kay, *Don Parker on Computer Crime*, INFOSECURITY NEWS, Nov./Dec. 1992, at 44.

<sup>428</sup> These issues are artfully considered in "Government's Opposition to Defendant's Motion to Dismiss the Indictment," *noted in* U.S. v. Morris, 728 F. Supp. 95 (N.D.N.Y. 1990), *aff'd.*, 928 F.2d 504 (2d Cir.), *cert. denied*, \_ U.S. \_, 112 S. Ct. 72 (1991).

<sup>429</sup> One problem with proposed "unauthorized use" legislation is concern that, in practice, authorization is too discretionary and that persons would be subject to prosecution that society does not desire to prosecute. For example, consider a situation where two (or more) engage in computer-based joint authorship of a document; halfway through the project, one of the collaborators deletes the other's contribution without authorization. This form of conduct would be difficult to exclude from an unauthorized access statute, and yet is precisely what we would not want to criminalize. *See* Telephone Interview with S. Charney, Esq., U.S. Dep't of Justice (Aug. 17, 1993).



- Whether criminal statutes that require proof of loss or destruction to information should also require intent to cause loss or destruction or whether it should be satisfied upon a showing that the defendant intended merely to gain unauthorized access but in fact caused a loss.

The criminal enforcement option does exist and is strengthening for computer-based crime, although a corresponding international response lags.<sup>430</sup> The remainder of this section identifies criminal laws that are particularly relevant to FCA activities.<sup>431</sup> The first set of laws (discussed below) survey computer crime laws; the second surveys non-computer-specific laws that may support computer-based criminal liability. Consideration of both sets of laws provides fertile ground for future research and legal response.

## 2. Survey of Computer Crime Statutes

- 18 U.S.C. § 1030 (Computer Fraud and Abuse Act of 1986). Particularly relevant subsections of this Act are considered below.
- 18 U.S.C. § 1030(a)(5) "Altering, damaging, or destroying of information on federal-interest computers." This statute punishes anyone who:

intentionally accesses a Federal interest computer<sup>432</sup> without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in

---

<sup>430</sup> However, the need for international cooperation is imperative. See A. Bequai, *The U.S. Experience in Computer Crime*, PROCEEDINGS OF COMPSEC '92, 62, 68 (London Nov. 4-6, 1992). It must involve international organizations, national governments and the private sector. See M. Jones, *Dealing with computer misuse - the need for an international approach*, PROCEEDINGS OF COMPSEC '92, *supra*, at 475.

<sup>431</sup> See also, Food and Drug Administration, 57 Fed. Reg. 32,185 (July 21, 1992) (Request for Information and Comments concerning enforcement proceedings related to electronic identification, signatures and records).

<sup>432</sup> A federal interest computer is one that is:

(A) exclusively for the use of a financial institution or the United States Government or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affected the use of the financial institution's operation or the Government's operation of such computer; or

any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby

(A) causes loss to one or more others of a value aggregating \$1,000 or more during any one year period . . .

An infamous case under the Computer Fraud and Abuse Act is that of *United States v. Morris*,<sup>433</sup> where the government was not required to demonstrate that the defendant *intentionally* prevented authorized use and thereby to cause loss. Rather, "the intent requirement applied only to the accessing and not to the resulting damage."<sup>434</sup>

*Access* includes the use of computer resources, such as information contained within data bases or computer processing resources. Consequently, this statute, and other computer abuse statutes, may be inapplicable to FCA-based certificate and digital signature practices because they were developed to address *access* issues, whereas the FCA is primarily intended to serve message *authentication* and *integrity* purposes.<sup>435</sup> To the extent access control statutes do not provide a

---

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State . . .

18 U.S.C. § 1030(e)(2).

<sup>433</sup> 928 F.2d 504, 505 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991) (affirming conviction for violating 18 U.S.C. § 1030(a)(5)(A) and stating "Morris released into INTERNET [a 'worm' that eventually caused numerous] computers at various educational institutions and military sites to 'crash' or cease functioning").

<sup>434</sup> *Id.* at 506. The court reasoned as follows:

Congress expressed concern that the "knowingly" standard [in the 1984 Computer Fraud and Abuse Act] 'might be inappropriate for cases involving computer technology.' . . . The concern was that a scienter requirement of "knowingly" might encompass the acts of an individual "who inadvertently 'stumble[d] into' someone else's computer file or computer data," especially where such individual was authorized to use a particular computer.

*Id.* at 506, 507-508.

<sup>435</sup> Note that RFC 1421 (PEM Part I: Message Encryption and Authentication Procedures) (Feb. 1993) states:

Based on these principles, the following facilities are provided:

1. disclosure protection,
2. originator authenticity,



viable basis for FCA-related prosecution, forgery<sup>436</sup> and generic fraud<sup>437</sup> statutes also deserve further consideration:

- 
3. message integrity measures, and
  4. (if asymmetric key management is used) non-repudiation of origin, but the following privacy-relevant concerns are *not* addressed:
    1. *access control*

*Id.* at 5 (emphasis added).

ISO and domestic information security standards and guidelines present a confusing picture of these terms and, in particular, whether the term *access control* reasonably includes authentication and integrity protections. For example:

3.3.2 access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner . . .

3.3.7 authentication: see data origin authentication and peer entity authentication . . .

3.3.2.2 data origin authentication: the corroboration that the source of data received is as claimed . . .

3.3.40 peer-entity authentication: The corroboration that a peer entity in an association is the one claimed . . .

ISO 7498-2-1988(E).

Cf. GLOSSARY OF COMPUTER SECURITY TERMS, NCSC-TG-004, Version 1 (21 Oct. 1988) ("access control: The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with *controlled access* and *limited access*.").

The relationship between access/access control and authentication can be varied or confusing. Note that authentication is often a prerequisite to access: "[T]he authentication service may pass the results of authentication to the access control service, to be used by the access control service." INFORMATION RETRIEVAL, TRANSFER AND MANAGEMENT FOR OSI SECRETARIAT: USA (ANSI) ISO/IEC JTC1/SC21 Second CD 10181-2, § 9.1.

<sup>436</sup> See generally 36 AM. JUR. 2d §§ 6-14 (surveying the criminal acts of forgery).

<sup>437</sup> "A fraud claim must involve a false statement of a past or present material fact." *American Computer Truck Leasing v. Jack Farrell Implement Co.*, 763 F.

The statutes create a crime analogous to trespass but different in form, since they require no physical invasion of protected space.<sup>438</sup> The owner has a property right in the computer it controls and a right to exclude other persons. '[Trespass] statutes criminalize the entering and remaining on premises; . . . [c]omputer trespass . . . criminalizes the entry into the computer base.'<sup>439</sup> Despite the fact that trespass requires physical entry and electronic access does not, these statutes establish as a primary principle an expectation of protected control over the electronic environment parallel to control over physical environments.<sup>440</sup>

Although public key-based confidentiality services can provide, or contribute to, capabilities similar to access control, it is assumed that the FCA will not perform confidentiality services in its initial implementation.<sup>441</sup> Accordingly, the confidentiality avenue cannot be counted upon to support the criminalization of conduct on the basis of access alone.<sup>442</sup>

When all activity is undertaken within one state and where the computers involved are not otherwise *Federal interest computers*, the statute is inapplicable. This is problematic in that FCA-issued certificates will likely be used to support access to more than just "Federal interest computers" as defined under current law. Consequently, other applicable federal and state laws, deserve consideration.

---

Supp. 1473, 1485 (D. Minn. 1991) (citing *Dollar Travel Agency, Inc. v. Northwest Airlines*, 354 N.W.2d 880 (Minn. Ct. App. 1984)).

<sup>438</sup> Cf. *id.* at 1473 (trespass laws do not protect the owner of a computer against access to that computer by a third party).

<sup>439</sup> *State v. Olson*, 47 Wash. App. 514, 1 C.C.H. Computer Cases (C.C.H.) ¶ 45.039 (1987).

<sup>440</sup> *Nimmer & Krauthaus*, *supra* note 98, at 28-29.

<sup>441</sup> See Section IV.D., *supra* (Assumptions: "Availability"), where it is noted that the Digital Signature Standard does not provide for message content confidentiality.

<sup>442</sup> One security expert has suggested that access control-oriented statutes are "inapplicable" [to PEM and the FCA]. Telephone Interview with S. Kent, Chief Scientist, BBN (July 28, 1993).



- 18 U.S.C. § 1030(a)(2) "Fraudulent possession and use of access device."<sup>443</sup>

(a) Whoever-

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.)

- 18 U.S.C. § 1029 "Fraud and related activity in connection with computers."  
Sections 1029(a) of this law provide that anyone who:

(1) knowingly and with intent to defraud, produces, uses, or traffics in one or more counterfeit access devices;<sup>444</sup>

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

shall, if the offense affects interstate commerce, be punished . . . .

---

<sup>443</sup> The risks associated with "exceed(ing) authorized access" pursuant to § 1030(a)(2) are potentially mitigated by the security services provided by authentication certificates. See Section V.C.4., *supra*.

<sup>444</sup> An *access device* is "any card, plate, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." *id.* § 1029(e)(1). An *unauthorized access device* is an "access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." 18 U.S.C. § 1029(e)(3). A "counterfeit access device means any access device that is counterfeit, fictitious, altered, or forged or an identifiable component of an access device or a counterfeit access device." *Id.* § 1029(e)(2).

See *United States v. Lee*, 815 F.2d 550 (5th Cir. 1987) (rejecting vagueness challenge to § 1029 as applied to credit card numbers); *United States v. Brewer*, 835 F.2d 550 (5th Cir. 1987) (applying § 1029 to telephone calling codes). However, neither of these cases concerned *physical* devices.

This law may be particularly relevant where card technologies (e.g., "smart cards") are used in connection with FCA activities, such as to support authenticated transactions.<sup>445</sup> In a major computer crime case, many aspects of computer abuse laws were challenged and issues were raised as to whether the defendants should be charged with knowledge that user-ID/passwords are a means of account access under the statute.<sup>446</sup> The Government asserted that "defendant's familiarity with passwords as a type of 'account access' is clearly relevant in determining whether the statutory language is too vague."<sup>447</sup> "The question of whether section 1029 applies to the unauthorized use of computer passwords is an open one."<sup>448</sup>

---

<sup>445</sup> See Section IV.L. ("Assumptions:" "Use of Card Technologies"), *supra*. But see *United States v. Blackmon*, 839 F.2d 900, 913-914 (2d Cir. 1988). However, the extent to which First Amendment freedoms are implicated will affect the vagueness analysis.

<sup>446</sup> See Government's Memorandum of Law in Opposition to Defendants' Pre-Trial Motions, Feb. 13, 1993, *U.S. v. Julio Fernandez*, a/k/a "Outlaw;" John Lee, a/k/a/ "John Farrington," a/k/a/ "Corrupt," Mark Abene, a/k/a "Phiber Optik," Elias Ladopoulos, a/k/a "Acid Phreak;" and Paul Stira, a/k/a "Scorpion," No. 92 Cr. 563 (RO) (S.D.N.Y. 1993) (concerning unauthorized intrusion into N.Y. telephone computers and the infamous *Masters of Disaster* case).

<sup>447</sup> *Id.* at 14 (citing *Precious Metals Ass'n v. Commodity Future Trading Comm'n*, 620 F.2d 900, 907 (1st Cir. 1980); *Village of Hoffman Estates v. The Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 501 n.18 (1982)).

<sup>448</sup> S. Fishbein, *What Victims of Computer Crime Should Know and Do*, N.Y. L.J., Nov. 12, 1993, at 1, 3. Fishbein cites *United States v. McNutt*, 908 F.2d 561 (10th Cir. 1990):

The government contends that the electronic addresses in descramblers are a "means of account access" under § 1029(e)(1) because legitimate viewers who pay subscription fees to satellite television programmers provide a "free ride" to the users of cloned descramblers. In advancing this argument, however, the government has mistaken economic losses for actual monetary losses resulting from discrete transactions reflected in the company's accounting records. . . . As used in § 1029, an account constitutes "a formal record of debits and credits" . . . Unlike the unauthorized use of credit cards or long distance telephone access codes, use of cloned descrambler modules does not debit legitimate subscribers' accounts; no additional charges are accrued as a result of the unauthorized use . . . we find nothing in the plain wording, legislative history or judicial interpretation of § 1029 which would lead us to believe that Congress intended that statute to apply to anything other than direct accounting losses.



• 18 U.S.C. § 2701 "Unlawful Access to Stored Communications." This section of the Electronic Communications Privacy Act of 1986<sup>449</sup> prohibits anyone who:

(1) Intentionally accesses without authorization a facility through which an electronic communication service is prohibited; or

(2) Intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to wire or electronic communication while it is in electronic storage in such system . . .

• 18 U.S.C. § 1343 "Fraud by wire, radio, or television."<sup>450</sup>

Whoever, having devised or intended to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than \$1,000 or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.

### 3. Survey of Relevant Non-Computer-Specific Statutes

The following laws indirectly address, but bear upon, computer crime and abuse and may be important to the extent that access-based law fails to address public key and FCA requirements.

• 18 U.S.C. § 371 "Conspiracy to commit offense or to defraud United States."

---

*Id.* at 563-64. *Contra* United States v. Fernandez, No. 92 Cr. 563, 1993 WL 88197 (S.D.N.Y. Mar. 24, 1993).

<sup>449</sup> Title 1 of the Act prohibits the interception of wire, oral, or electronic communications. It defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic mechanical, or other device." 18 U.S.C. § 2510(4).

<sup>450</sup> See United States v. Riggs, 743 F. Supp. 556 (N.D. Ill. 1990), *noted in* United States v. Riggs, 967 F.2d 561 (11th Cir. 1992) (affirming separate conviction).

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

Conspiracy as a basis for FCA-related criminal prosecution should be considered, *e.g.*, with respect to: (i) conspiracy to defraud by the holders of split keys that control the FCA's certificate generation devices; (ii) conspiracy of a certificate applicant and a CA employee to issue a false certificate; and (iii) conspiracy of FCA employees to issue fraudulent CRLs or to fail to issue CRLs containing a particular certificate. Conspiracy laws have been useful in computer abuse prosecutions.

- 18 U.S.C. § 1001 "Statements or entries generally."

Whoever, in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

- 18 U.S.C. § 1031 "Major fraud against the United States."

(a) Whoever knowingly executes, or attempts to execute, any scheme or artifices with the intent-

(1) to defraud the United States; or

(2) to obtain money or property by means of false or fraudulent pretenses, representations, or promises, in any procurement of property or services as a prime contractor with the United States or as a subcontractor or supplier on a contract win which there is a prime contract with the United States, if the value of the contract, subcontract, or any constituent part thereof, for such property or services is \$1,000,000 or more shall . . . be fined not more than \$1,000,000, or imprisoned not more than 10 years, or both.



- 18 U.S.C. § 1342 "Fictitious name or address."

Whoever, for the purpose of conducting, promoting, or carrying on by means of the Postal Service, any scheme or device mentioned in section 1341 of this title or any other unlawful business, uses or assumes, or requests to be addressed by, any fictitious, false, or assumed title, name, or address or name other than his own proper name, or takes or receives from any post office or authorized depository of mail matter, any letter, postal card, package, or other mail matter addressed to any such fictitious, false, or assumed title, name, or address, or name other than his own proper name, shall be fined not more than \$1,000 or imprisoned not more than five years, or both.<sup>451</sup>

- 18 U.S.C. § 1341 "Fraud and swindles."

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose or, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined not more than \$1,000 or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.

- 18 U.S.C. § 1505 "Obstruction of proceedings before departments, agencies, and committees."

Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States . . . shall be fined not more than \$ 5,000 or imprisoned not more than five years, or both.

---

<sup>451</sup> This section should be considered in light of USPS involvement in CA activities. *See* Section VII.A.4.a., *infra*; *cf.* *Strauss v. United States*, 516 F.2d 980 (C.A. Ill. 1975).

• 18 U.S.C. §§ 1961 *et seq.* "Federal Racketeer Influenced and Corrupt Organizations [(RICO)] Act."<sup>452</sup> Section 1962 prohibits the following activities under RICO:

(a) It shall be unlawful for any person who has received any income derived, directly or indirectly, from a pattern of racketeering activity or through collection of an unlawful debt in which such person has participated as a principal within the meaning of section 2, title 18, United States Code, to use or invest, directly or indirectly, any part of such income, or the proceeds of such income, in acquisition of any interest in, or the establishment or operation of, any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce. A purchase of securities on the open market for purposes of investment, and without the intention of controlling or participating in the control of the issuer, or of assisting another to do so, shall not be unlawful under this subsection if the securities of the issuer held by the purchaser, the members of his immediate family, and his or their accomplices in any pattern or racketeering activity or the collection of an unlawful debt after such purchase do not amount in the aggregate to one percent of the outstanding securities of any one class, and do not confer either in law or in fact, the owner to elect one or more directors of the issuer.

(b) It shall be unlawful for any person through a pattern of racketeering activity or through collection of an unlawful debt to acquire or maintain, directly or indirectly, any interest in or control of any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.

(c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt.

(d) It shall be unlawful for any person to conspire to violate any of the provisions of subsections (a), (b), or (c) of this section.

Several legislative proposals to curtail the scope of RICO's civil provisions are anticipated to be introduced in Congress that may affect RICO's potential impact on the FCA.<sup>453</sup>

---

<sup>452</sup> Cf. *American Computer Trust Leasing v. Jack Farrell Implement Co.*, 763 F. Supp. 1473 (rejecting RICO claim).

<sup>453</sup> The proposals include: precluding punitive damages where treble damages are available; introducing a more restrictive statute of limitations; removing "enterprise" from liability under certain circumstances; requiring "active participation" in § 1962(c) where a person "conduct[s]" an enterprise's affairs consistent with *Reves v. Ernst & Young*, 61 U.S.L.W. 4207 (1993); and to require injury from overt acts prohibited by RICO. *ABA Denounces New Discovery Rule, Accredits Lawyer Specialization Agencies*, 62 U.S.L.W. 2097 (Aug. 17, 1993).



- 18 U.S.C. § 641 "Public money, property or records."

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract of the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted [shall be fined] . . .

- 18 U.S.C. § 1361 "Government property or contracts."

Whoever willfully injures or commits any depredation against any property of the United States, or of any department or agency thereof, or any property which has been or is being manufactured or constructed for the United States, or any department or agency thereof, shall be punished as follows . . .

- 18 U.S.C. § 1362 "Communication lines, stations or systems."

Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willful or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, shall be fined not more than ten year, or both.

This law may become particularly useful due to the increasing use of wireless data communications.<sup>454</sup>

---

<sup>454</sup> See, e.g., Andrews, *F.C.C. Clearing Airwaves For an Era Without Wires*, N.Y. TIMES, Sept. 20, 1993, at 1, 10 (quoting A. Sikes, prior F.C.C. Chairman: "This will shake the foundation of the entire telecommunications industry.").

• 18 U.S.C. § 2071 "Concealment, removal, or mutilation generally."

(a) Whoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or, with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States, shall be fined not more than \$2,000 or imprisoned not more than three years, or both.

(b) Whoever, having the custody of any such record, proceeding, map, book, document, paper, or other thing, willfully and unlawfully conceals, removes, mutilates, obliterates, falsifies, or destroys the same, shall be fined not more than \$2,000 or imprisoned not more than three years, or both; and shall forfeit his office and be disqualified from holding any office under the United States.

• 18 U.S.C. § 2314 "Transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting."

Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of \$5,000 or more, knowing the same to have been stolen, converted or taken by fraud; or

Whoever, having devised or intended to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person or persons to travel in, or to be transported in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of \$5,000 or more; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any falsely made, forged, altered, or counterfeited securities or tax stamps, knowing the same to have been falsely made, forged, altered, or counterfeited; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any traveler's check bearing a forged countersignature; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce, any tool, implement, or thing used or fitted to be used in falsely making, forging, altering, or counterfeiting any security or tax stamp, or any part thereof –

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

Note that Congress chose the preponderance standard when it created substantive causes of action for fraud.<sup>455</sup>

---

<sup>455</sup> See *Grogan v. Garner*, 498 U.S. 279, 288 (1991) (holding that defrauding creditor not required to prove claim by clear and convincing evidence).



• 15 U.S.C. §§ 78dd-1 *et seq.* "Foreign Corrupt Practices Act of 1977."<sup>456</sup> This Act imposes record keeping requirements on all publicly held companies and requires the establishment of appropriate internal accounting controls, among other requirements.

The Federal Sentencing Guidelines may also require review in light of the potential catastrophic harms that root key compromise and other potential compromises could create. Such review might be undertaken in a fashion not unlike the recent revision of the Guidelines to add penalty "points" for privacy breaches.<sup>457</sup> Finally, the computer crime laws of other countries should be carefully evaluated, including the sufficiency of extradition treaties.<sup>458</sup>

---

<sup>456</sup> 91 STAT. 1495 as amended.

<sup>457</sup> Also, *see* U.S. Sentencing Commission's proposed guideline for the Computer Fraud and Abuse Act, submitted by the Electronic Frontier Foundation and the Society for Electronic Access, *cited in* 58 Fed. Reg. 67,522. *See generally* Sentencing Reform Act, 28 U.S.C. §§ ww991-998 (creating a commission as an independent entity within the Judicial Branch with powers to promulgate sentencing guidelines).

<sup>458</sup> *See* M. Jones, *supra* note 430; *see also* Canadian Criminal Law Amendment Act 1985 (covering computer-based interception, modification and destruction); Australian Capital Territory Crimes (Amendment) Ordinance (No. 4) 1985; U.K. Computer Misuse Act 1990.

#### 4. Summary

The foregoing survey suggests that computer crime and abuse laws do not clearly and convincingly provide the necessary tools for responsive prosecutorial action, and as such, may have the effect of impeding public confidence in the FCA. Interviews and research by the author did not inspire confidence that the legislature and criminal justice system has commenced appropriate consideration of these issues with a view toward framing a cogent response. This Report includes a responsive recommendation concerning computer crime laws.<sup>459</sup>

---

<sup>459</sup> Section X.N., *infra*.

As a closing note to this section on criminal law, the following unsettling quotations provide a sobering picture of the importance and urgency of the criminal law reform issues. Futurist Alan Toffler stated, "we know a former senior intelligence official who says, '[g]ive me 1 billion and 20 people and I'll shut America down. I'll shut down the Federal Reserve, all ATMs; I'll desynchronize every computer in the country.' I come away persuaded that we are going to see infoterrorism not just by hackers playing games, but by countries or criminal syndicates that learn to do this stuff very effectively." Toffler Interview, INFORMATION WEEK, Jan. 10, 1994, at 50.

Tim Worth, Undersecretary of State for Global Affairs remarked, "we have a problem that is accelerating far beyond the ability of our current institutions"; Senator John Kerry stated "organized crime [is] the new communism, the new monolithic threat"; Roy Godson, National Strategy Info. Ctr., stated, "[organized crime] is an iceberg; nobody knows the size of it. . . . [it] has contributed 'to form a new space for organized crime: a vast hunting ground with no fixed borders and with an entry permit available on to the cruel and deadly'." Elliot, *Global Mafia*, NEWSWEEK, Dec. 13, 1993, at 24.



## VII. FCA INFRASTRUCTURE - PROPOSALS AND PARADIGMS

Current proposals for the FCA include lodging it within a dependent or independent agency of the federal government and contracting with the private sector for the provision of some limited FCA services. This section surveys various requirements of such proposals, discusses liability issues peculiar to federal activities and evaluates certain agencies as potential candidates to provide FCA services.

### A. THE FEDERAL GOVERNMENT AS PROVIDER OF FCA SERVICES

Placement of the FCA within a dependent or independent agency of the federal government would provide an opportunity to establish the FCA by means of legislation or, at a minimum, comprehensive regulation. Accordingly, the FCA could be written on a blank slate and, subject to the political pressures of the moment, could be fashioned so as to conform with virtually any liability regime that may be desired. The following analysis considers these issues and examines a number of existing FCA candidates and the liability regimes applicable thereto.

#### 1. Constitutional Issues

The FCA raises several constitutional issues that should be taken into consideration in designing its infrastructure, including threats to principles of the separation of powers and individual liberties.<sup>460</sup> Constitutional authorization for

---

<sup>460</sup> Some constitutional issues associated with the implementation of "Clipper-Chip" "key escrow" proposal are also relevant to the FCA. It is recognized, however, that Clipper-Chip keys are not public keys:

A "key-escrow" will be established to ensure that the "Clipper-Chip" is used to protect the privacy of law-abiding Americans. Each device containing the chip will have two unique "keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorization to conduct a wiretap.

Statement by the Press Secretary, White House (Apr. 16, 1993). *See generally* Section VIII.C., *infra* ("Escrow and Other Legal Agents"); NIST, *A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES)*, 58 Fed. Reg. 40,791 (July 30, 1993).

the undertaking of FCA activities by the federal government likely exists under one or more of the plenary powers enumerated in Article 1, Section 8 of the Constitution of the United States.<sup>461</sup> A finding that the FCA is unconstitutional would have predictable consequences for its viability: its demise.<sup>462</sup>

---

In considering these escrow issues in light of the roles of the FCA, at least where it undertakes key generation (*see* Section V.A.2.h., *supra*), one security expert notes that discrete and identifiable "escrow accounts provide significant targets and that all modern systems seek as one of the primary goals to reduce their attractiveness as targets. I would reject this particular mechanism on this issue alone." E-mail from John Lowry, BBN, to Michael Baum (June 17, 1993).

<sup>461</sup> The United States Constitution vests Congress, *inter alia*, with the following powers:

The Congress shall have power . . .

To regulate Commerce with foreign nations, and among the several states . . .

To coin money . . .

To provide for the punishment of counterfeiting the securities and current coin of the United States:

To establish post-offices and post-roads:

To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries . . .

- And

To make all laws which shall be necessary and proper for carrying into execution the foregoing powers, and all other powers vested by this Constitution in the government of the United States, or in any department or officer thereof.

U.S. CONST. art. I, § 8. The scope of the Commerce Clause, in particular, is broad. "Contemporary commerce clause doctrine grants Congress such broad power that judicial review of the affirmative authorization for congressional action is largely a formality." L. TRIBE, *AMERICAN CONSTITUTIONAL LAW* 316 (2d ed. 1988); *cf.* "If anything that will take you across a state line is an 'instrumentality of commerce,' then there is justification for Congress to regulate anything done on a bicycle or, for that matter, on foot." *U.S. v. Cortner*, No. 3:93-00009 (U.S. D.Ct., M.D. Tenn., Oct. 19, 1993) (concerning constitutionality of the "Anti-Car Theft Act").

<sup>462</sup> The mandatory versus permissive use of the FCA [*see* Section IV.G. ("Assumptions:" "Privilege; Not a Right"), *supra*.] and Clipper share certain issues of potential constitutional dimension. One commentator has segmented FCA use as follows: (i) mandatory government use, (ii) voluntary government use, (iii) mandatory government-private use, (iv) mandatory private use, and (v) voluntary private use. Memo from F. Sudia, Bankers Trust, to Michael Baum (Nov. 17, 1993) (on file with Independent Monitoring). Note that the federal government has sought to minimize constitutional challenge of the Clipper



## a. SEPARATION OF POWERS

There is a slight risk that placing the FCA within the federal government could threaten the constitutional separation of powers between the executive, judicial and legislative branches of the government.<sup>463</sup> The danger is illustrated by the following:

*Hypothetical:* Assume that the FCA serves each branch of the Federal Government and is operated by an entity under the control or supervision of the Executive Branch, such as the General Services Administration. Assume also that a crisis similar to "Watergate" occurs and that acts of the President are challenged as unconstitutional and/or criminal. An investigation ensues by a special prosecutor resulting in litigation and a constitutional crisis.

*Case 1:* Not inconsistent with Nixon Administration conduct, assume the President's Chief of Staff orders revocation of the public key certificates issued by the FCA to the Supreme Court and the lower federal courts.<sup>464</sup> The *hot*

---

initiative by asserting that its mandatory use will be restricted to official government business.

<sup>463</sup> Separation of powers is fundamentally an implication of the following specific grants of autonomy: "All legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives," U.S. CONST. art. I, § 1; "The executive power shall be vested in a President of the United States of America," *Id.* art. II, § 1; "The judicial power of the United States, shall be vested in one supreme court, and in such inferior courts as the Congress may, from time to time, ordain and establish." *Id.* art. III, § 1. Perhaps certain constitutional concerns are tempered by FCA constitutional parallels to federal wiretap procedures. *See infra* note 466; *cf.* A. Toffler, *Shock Wave (Anti) Warrior*, WIRED, Nov. 1993, at 61, 122 ("We strongly believe in the separation of powers, but there are multiple ways to separate powers. The idea that they are separated into a legislature, a judiciary, and an executive is only one way of slicing it. You've got to ask yourself what-if questions. What are alternative ways of going about this? Americans seem to think that our system is the only imaginable system.").

<sup>464</sup> Arguably, in a political crisis, the Executive Branch's issuance of CRLs covering significant portions of the judiciary's certificates would be met by non-observance of the CRL(s) and continued operation, under emergency conditions, using the last "known good" CRL. This would obviously, nonetheless, result in a loss of time, effort and a degree of certainty and confidence in the system that would not easily be recovered.

*listing of the federal courts' certificates destroys or impedes assurances of authenticity, integrity and confidentiality necessary to the proper operation of the Judiciary Branch.*

*Case 2: Not inconsistent with Nixon Administration conduct, assume the President's Chief of Staff illegally seeks to obtain confidential communications sent to certain members of Congress. To do so, the Chief of Staff orders the FCA to publish fictitious public keys for those members of Congress so that*

---

Confidentiality within the Judicial Branch is an important value:

Although it is difficult to find authorities discussing the existence of a duty on the part of federal judges to guard the confidentiality of their communications with their colleagues, that is undoubtedly because "its existence and validity has been so universally recognized. Its source is rooted in history and gains added force from the constitutional separation of powers of the three departments of government."

Nixon v. Sirica, 487 F.2d 700, 740 (D.C. Cir. 1973), (explicated in United States v. Aguilar, 994 F.2d 609 (9th Cir. 1993), *on reh'g*, 1994 WL 133074 (Apr. 19, 1994)).

Numerous variations on this theme are possible. Thus, the same problem would occur if the inferior federal courts were issued certificates by the Supreme Court, which had itself been issued a certificate by, or had otherwise registered its CA policy with, the FCA's registration authority. Comparable examples, in this case a challenge to federalism, could be given where the FCA issues a CRL for a state government entity, thereby impairing or infringing upon that government's powers. Such conduct might violate the 10th Amendment to the Constitution: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people;" or the 11th Amendment: "The judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States, by citizens of another state, or by citizens or subjects of any foreign state."

Even if the States operate their own root certification authorities (a highly unlikely possibility), they would likely need to communicate securely with other entities within the federal government (arguably by cross-certification. *But see* Section V.A.6.b. *supra* (concerning issuing certificates for cross-certification purposes). Note that in such a situation, either government would then have the power (if not the right) to revoke the cross-certification. State governments attempting to cooperate with a federal probe would be unable to communicate with federal authorities and *vice-versa*.



FCA operatives could decrypt the communications of persons who have been duped into relying on the fictitious certificates.<sup>465</sup>

These examples raise substantial issues concerning whether there should (or can or must) be a single government-wide FCA or, instead, at least one independent (root) FCA entity for each of the three branches.<sup>466</sup> The courts have regularly struck down congressional enactments for separation of powers violations.<sup>467</sup>

Another facet of separation of powers jurisprudence is that of proper delegation. An important reason for concentrating analysis on "delegation" issues is the need for both actual and apparent trustworthiness, which, in turn, require independence and impartiality.<sup>468</sup>

---

<sup>465</sup> Case 2 is not so compelling as Case 1 because members would soon notice either that they could not decrypt messages or that they were no longer receiving messages. However, operatives could also fabricate certificates for members and issue signed messages on their behalf or, better yet, issue court orders requiring the release of information, etc. While the hypothetical focuses on Executive Branch impropriety, similar threats pertain within the Legislative and Judicial Branches of government as well.

<sup>466</sup> Without reaching the underlying constitutional permissibility, consider the extent to which a Clipper-like dual escrow scheme, *i.e.*, a two-component escrow arrangement, satisfies the needs of a tripartite government structure. Perhaps a *root* should be established for each branch, and its two components escrowed with the root of each other branch (or, in the case of the FCA, trifurcate the authority to initiate a CRL by the highest FCA authority among each branch of the government). However, any such scheme presents subtle and inherent risks. A mitigating argument is based upon the observation that current federal wiretap warrants issued pursuant to the federal wiretap statute, 18 U.S.C. § 2518, are undertaken without comparable controls. *See, e.g., Rotenberg, Statement of CPSR Washington Office before the Computer System Security Advisory Board*, June 1992 (noting federal wiretap restrictions and problems).

<sup>467</sup> Among the more notorious cases of the previous decade are the following: *Bowsher v. Synar*, 487 U.S. 714 (1986) (congressional power to remove executive branch officer); *I.N.S. v. Chadha*, 462 U.S. 919 (1983) ("legislative veto" over individual determinations by agency); *Northern Pipeline Constr. Co. v. Marathon Pipe Line Co.*, 458 U.S. 50 (1982) (vesting "judicial Power of the United States" in tribunals lacking tenure and salary protections). *See generally Strauss, Formal and Functional Approaches to Separation-of-Powers Questions: A Foolish Inconsistency*, 72 CORNELL L. REV. 488 (1987).

<sup>468</sup> This issue was recently raised when a federal judge stated that the Clinton administration had "dilly-dallied" in carrying out its orders to preserve "nearly

Assuming that Congress has the authority pursuant to the Commerce Clause or one or more of its other plenary powers to enact FCA legislation, or that Congress already has enacted legislation sufficiently broad in scope to authorize forays into this area,<sup>469</sup> the foregoing hypotheticals demonstrate the need for sensitivity to issues of delegation. These issues fall into three categories: delegation of FCA authority to the Executive Branch; delegation of FCA authority to private entities; and the implications for separation of powers principles of vesting what will likely amount to substantial *power* (in the brute sense) over the legislative and judicial branches (in a single executive branch agency or its delegee).

Delegation of regulatory authority to the Executive Branch is a familiar phenomenon posing few problems. Although the text of the Constitution itself suggests a number of areas in which legislative power is not delegable,<sup>470</sup> legislation enacted pursuant to, for example, the Commerce and Post Office Clauses is emphatically not among them. Two issues should be raised, however. First, and least troublesome, is the requirement that "delegated power include at least roughly intelligible 'standards' to guide the delegated party. . . ."<sup>471</sup> This scrutiny, however, typically takes the form of statutory, rather than constitutional, interpretation.<sup>472</sup> Accordingly, a clear statement on the part of Congress,<sup>473</sup> perhaps together with evidence in the legislative history that Congress had evaluated potential constitutional infirmities or dangers of the FCA, would likely be sufficient to immunize the FCA from attack on grounds of improper delegation to the Executive Branch.

---

6,000 computer tapes of White House and National Security Council," E-mail transmissions under the Bush and Reagan Administrations: "This case has been one of avoidance of responsibility by the government bureaucracy." *Judge Calls Administration Lax on Predecessors' Computer Records*, N.Y. TIMES, June 9, 1993, at A18; see *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993).

<sup>469</sup> See, e.g., Sections VII.A.4., *infra* (discussing authority generally as well as existing authority of the United States Postal Service and the Federal Reserve to establish FCA operations).

<sup>470</sup> See *TRIBE*, *supra* note 461, at 362-63.

<sup>471</sup> *Id.* at 364.

<sup>472</sup> See *id.* at 365.

<sup>473</sup> See *id.* at 366 n.14.



Use of an independent contractor to the federal government for the provision of FCA services raises the problem of "attempts to endow private decision making with coercive authority over others."<sup>474</sup> Given the constitutional sensitivity of certain aspects of the FCA, the only indisputable avoidance of this problem would be to remove all or virtually all components of private decision making from the scope of duties under the FCA contract. To the extent that certification is or becomes an interest worthy of constitutional protection,<sup>475</sup> and elements of discretion are permitted to intrude upon FCA operations and substantive decisions, the problem may become a substantial one.<sup>476</sup>

The final issue is the one posed by the hypotheticals. Although no case has been found which addresses the permissibility of agency authority having such a formal and direct impact on the legislative and judicial branches as the FCA is contemplated to possess, it would perhaps be instructive to review the structural independence of two "independent" government establishments: the United States Postal Service<sup>477</sup> and the Board of Governors of the Federal Reserve System.<sup>478</sup>

---

<sup>474</sup> *Id.* at 368. Floating somewhere between delegation to the Executive Branch and delegation to private parties is the problem of delegation to quasi-governmental entities. Unless some such entity, notably the United States Postal Service or the Board of Governors of the Federal Reserve Board, can make a plausible claim to have existing authority to undertake FCA operations, however, Congress would be forced to act either to create a new entity or to assign new responsibilities to an existing one. In either case, however, the problem is not analytically different from delegation to a purely governmental agency.

<sup>475</sup> See Section IV.G., *supra* ("Assumptions:" "Privilege, Not a Right").

<sup>476</sup> Discretionary acts may include determining which entities qualify (perhaps based on accreditation procedures) to serve as CAs, PCAs, etc.

<sup>477</sup> "There is established, as an *independent establishment* of the executive branch of the Government of the United States, the United States Postal Service." 39 U.S.C. § 201 (emphasis added).

<sup>478</sup> The examination of these two entities is particularly useful, for two reasons. First, they are both serious candidates to provide FCA services. Second, it is not difficult to imagine methods that might be used by the Federal Reserve System or the United States Postal Service to disrupt or to intrude on the respective "businesses" of the legislative and judicial branches.

Although the Federal Reserve System, made up of a series of individual Federal Reserve Banks, is an operating agency of the federal government,<sup>479</sup> it is governed in a manner that is purposefully independent from the control of the executive, legislative, or judicial branches of the federal government. Similarly, the United States Postal Service is governed by a Board of Governors. These institutions are discussed in greater detail below.<sup>480</sup>

## **b. FCA Threats to the Constitutional Rights of Persons**

This subsection considers certain potential threats to the Bill of Rights from the FCA. This discussion is intended simply as a brief survey of issues for further consideration.

### **Freedom of Speech - 1st Amendment**

The First Amendment expressly protects freedom of speech.<sup>481</sup> Because difficulty of access to certificates may impede a citizen's right to communicate, or to "speak," the regulation of certificates could amount to the regulation of speech. According to a recent Supreme Court decision, "[t]he government may regulate speech in order to promote a compelling state interest if it employs the least restrictive means to further that interest."<sup>482</sup> Both content-specific and content-neutral restriction issues are raised by certificate regulation or revocation.

---

<sup>479</sup> See *Federal Reserve Bank of Minneapolis v. Register of Deeds for Delta County*, 284 N.W. 667, 288 (Mich. 1939).

<sup>480</sup> See Sections VII.A.4.a. and VII.A.4.b., *infra*.

<sup>481</sup> "Congress shall make no law . . . abridging the freedom of speech or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." U.S. CONST. amend. I. Also, FCA restrictions on the issuance of "COI" (Community of Interest) [see Section V.A.3.f., *supra*] certificates could jeopardize constitutionally protected freedom of assembly.

<sup>482</sup> *Sable Communications of Cal., Inc. v. F.C.C.*, 492 U.S. 115, 126 (1989) (citing *United States v. Aguilar*, 994 F.2d 609 (9th Cir. 1993), *on reh'g*, 1994 WL 133074 (Apr. 19, 1994)).



## Searches and Seizures - 4th Amendment

Because of the FCA's critical position in the communications infrastructure, it could facilitate electronic "unreasonable searches and seizures" by law enforcement authorities. To the extent that improper operation of the FCA impedes on "[t]he right of the people to be secure in their persons, houses, [and] papers," and provides an avenue to undertake "unreasonable searches and seizures," the FCA could be used to violate the Fourth Amendment. An obvious threshold question is the extent to which the unique security afforded by encryption technology creates or elevates any "expectation of privacy" in FCA-facilitated communications or in CRD furnished to the FCA. Thus, for example, it is clear that "wire-tapping" of phone conversations implicates the Fourth Amendment.<sup>483</sup> However, it is also relatively clear that an individual has *no* expectation of privacy in records compiled by the telephone company of numbers dialed, length of calls and the like.<sup>484</sup> Where the FCA's activities fall along this spectrum will, of course, need to be the subject of judicial analysis.

## Privacy

Although no right of privacy is expressly enumerated in the U.S. Constitution, there is a significant basis for viewing privacy as an implied constitutional right.<sup>485</sup> While privacy is largely legislated *sectorally*,<sup>486</sup> other laws create a compelling basis for the FCA to treat privacy in a constitutionally protected fashion. Congressman Edward J. Markey recently noted that Americans should

---

<sup>483</sup> See *United States v. United States Dist. Court*, 407 U.S. 297 (1972); *United States v. Katz*, 389 U.S. 347 (1967); *cf.* 18 U.S.C. §§ 2510 *et seq.* (regulating and, for the most part, prohibiting "wire-taps" and other interceptions of electronic communications). The Electronic Communications Privacy Act of 1987 is discussed in Section VI.G., *supra*.

<sup>484</sup> See *Smith v. Maryland*, 442 U.S. 735 (1979).

<sup>485</sup> The classic case, of course, is *Griswald v. Connecticut*, 381 U.S. 479 (1965). See *generally* Computer Professionals For Social Responsibility, The Third CPSR Cryptography and Privacy Conference Source Book, June 7, 1993.

<sup>486</sup> That is, most legislation addressing privacy is limited to a sector of human activity, such as medical records or credit reporting, rather than providing comprehensive privacy protections. *But cf.* 5 U.S.C. § 552a (the Privacy Act) (providing a comprehensive prohibition on governmental release of personal information), which is discussed at Section VII.A.3.d., *infra*.

have "the right to protect their privacy through any form of encryption available to them."<sup>487</sup>

## 2. Authorization to Expend Funds

As illustrated in the immediately foregoing discussion, the federal government is one of limited powers. In addition to limits imposed on Congress, the Constitution also places limits on the Executive Branch. A critical theoretical and practical consideration in the commencement of any new program upon Executive Branch initiative is that of authority or ability to pay for it. This is as true for the FCA as for any other program.<sup>488</sup>

The Constitution unambiguously vests the "power of the purse" in Congress: "No Money shall be drawn from the Treasury but in consequence of appropriations made by law. . . ." <sup>489</sup> Congress has exercised this "negative authority" principally by means of two statutes: 41 U.S.C. § 11<sup>490</sup> and 31 U.S.C. § 1341.<sup>491</sup> Although it should be obvious, it bears noting that the foregoing implies:

---

<sup>487</sup> Edward J. Markey, Speech to the National Computer Ethics Conference (quoted in INFORMATION WEEK, May 17, 1993, at 62).

<sup>488</sup> The "Clipper-Capstone" initiative is reportedly being financed out of forfeiture proceeds made generally available for crime-control programs. Accordingly, existing rationales for "Clipper-Capstone" bear little legal or factual relevance to the FCA in this regard.

<sup>489</sup> U.S. CONST. art. I, § 9, cl. 7.

<sup>490</sup> "[N]o contract or purchase on behalf of the United States shall be made unless the same is authorized by law or is under an appropriation adequate to its fulfillment." 41 U.S.C. § 11(a) ("Adequacy of Appropriations Act").

<sup>491</sup> This statute provides, in relevant part, as follows:

(1) An officer or employee of the United States Government . . . may not -

(A) make or authorize an expenditure or obligation exceeding an amount available in an appropriation or fund for the expenditure or obligation;

(B) involve [the] government in a contract or obligation for the payment of money before an appropriation is made unless authorized by law . . . .



[A]n agency may not expend public funds or incur a liability to do so on the basis of a regulation, unless the regulation is implementing authority given by law. A regulation purporting to create a liability on the part of the government not supported by statutory authority is invalid and not binding on the government . . .<sup>492</sup>

The limits Congress has placed on expenditures operate on two distinct activities: the actual payment of funds and the making of contracts therefore. Frequently, contracts are made pursuant to lawful authority without a corresponding appropriation for payment. In such cases, Congress makes what are called "liquidating appropriations."<sup>493</sup>

Although interpreting appropriations statutes is not conceptually different from interpreting other statutes, Congress has provided a number of over-arching principles. First, appropriations laws are to be narrowly construed:

A law may be construed to make an appropriation out of the Treasury or to authorize making a contract for the payment of money in excess of an appropriation only if the law specifically states that an appropriation is made or that such a contract may be made.<sup>494</sup>

Also, "[a]n appropriation in a regular, annual appropriation law may be construed to be permanent or available continuously only if the appropriation . . . expressly provides that it is available after the final year covered by the law in which it appears."<sup>495</sup>

Once the scope of a general or specific appropriation has been determined, federal law further provides that "Appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law."<sup>496</sup>

---

31 U.S.C. § 1341(a).

<sup>492</sup> 1 U.S. GEN. ACCOUNTING OFFICE, PRINCIPLES OF FEDERAL APPROPRIATIONS LAW 3-9 to -10 (2d ed. 1991) [hereinafter PRINCIPLES] (citing *Atchison, T & SF RR Co. v. U.S.*, 55 Ct. Cl. 339 (1920); *Holland-American Line v. United States*, 53 Ct. Cl. 522 (1918); *Ill. Central RR Co. v. United States*, 52 Ct. Cl. 53 (1917)).

<sup>493</sup> 1 PRINCIPLES, *supra* note 492, at 2-5 to -6.

<sup>494</sup> 31 U.S.C. § 1301(d).

<sup>495</sup> *Id.* § 1301(c)(2).

<sup>496</sup> *Id.* § 1301(a). Title 31, section 3529, provides a procedure by which an agency official may request an advisory opinion from the Comptroller General respecting the propriety of a given disbursement. *Id.* § 3529. Such advisory opinions are binding on government. 1 PRINCIPLES, *supra* note 492, at 1-27 (citing, *inter alia*,

"The power to 'reprogram' (i.e., to "utiliz[e] funds in an appropriation account for purposes other than those contemplated at the time of appropriation . . . [to] shift [ ] funds from one object to another *within* an appropriation") is implicit in an agency's responsibility to manage its funds; no statutory authority is necessary."<sup>497</sup> This position does not appear to be supported by decided cases.

Also, Congress may, of course, ratify the unauthorized expenditure of funds retroactively.<sup>498</sup> Significantly, this power of ratification has been used to support experimentation by the former Post Office Department in innovative methods of transporting mail.<sup>499</sup>

An important issue that will surely arise in the context of a quasi-commercial enterprise such as the FCA is contemplated (in part) as being the status of funds received in the ordinary course of operations. In brief, section 3302(b), with exceptions not relevant to the present inquiry, provides that "an official or agent of the Government receiving money for the government from any source shall deposit the money in the Treasury as soon as practicable without deduction for any charge or claim."<sup>500</sup> The practical import of this provision is that, absent Congressional authority to the contrary, "Once money is deposited into a "miscellaneous receipts account, it takes an appropriation to get it back out."<sup>501</sup>

Finally, it is to be noted that the federal government operates under a presumption of self-insurance, the so-called "Self-Insurance Rule." "In the absence of express statutory authority to the contrary, appropriations funds are not available for the purchase of insurance to cover loss or damage to government property or the liability of government employees."<sup>502</sup> Although it has been

---

United States *ex rel.* Skinner & Eddy Corp. v. McCarl, 275 U.S. 1, 4 n.2 (1927); St. Louis, B & M RR Co. v. United States, 268 U.S. 169, 174 (1925); United States v. Standard Oil Co., 545 F.2d 624, 637-38 (9th Cir. 1976)).

<sup>497</sup> See 1 PRINCIPLES, *supra* note 492, at 2-25 (emphasis added).

<sup>498</sup> *Id.* at 2-52 (citing *Green v. McElroy*, 360 U.S. 474, 504-06 (1959); *Ex parte Endo*, 320 U.S. 283, 303 n.24 (1944); *Brooks v. Dewar*, 313 U.S. 354, 360-61 (1941); *Swayne & Hoyt, Ltd. v. United States*, 300 U.S. 297, 301-03 (1937)).

<sup>499</sup> See *Atchison, T & SF Ry. Co. v. Summerfield*, 229 F.2d 777 (D.C. Cir. 1955), *cert. denied*, 351 U.S. 926 (1956).

<sup>500</sup> 31 U.S.C. § 3302(b).

<sup>501</sup> 2 PRINCIPLES, *supra* note 492, at 6-107 (1992).

<sup>502</sup> *Id.* at 4-144.



argued that exceptions to the "Self-Insurance Rule" exist for situations where the economy of self-insurance would be lacking;<sup>503</sup> where "sound business practice" dictates to the contrary;<sup>504</sup> where the purchase of insurance would make available "services or benefits not otherwise available";<sup>505</sup> for government corporations;<sup>506</sup> and for bonding notaries public,<sup>507</sup> all of which situations may support the FCA infrastructure,<sup>508</sup> the "Self-Insurance Rule" will have to be addressed if it is decided that the purchase of private insurance should be part of FCA operations.

An important potential source for FCA funding is the so-called "Information Technology Fund" ("the Fund")<sup>509</sup> to which "[t]here are authorized to be appropriated . . . such sums as may be required," "without fiscal year limitation."<sup>510</sup> The fund is made up of funds appropriated and equipment acquired pursuant to prior telecommunications and automatic data processing initiatives.<sup>511</sup> In general, the Fund is "available for expenses . . . for efficiently providing information technology resources to Federal agencies . . . ."<sup>512</sup> Clearly a search for resources with which to implement an FCA should consider this fund.

---

<sup>503</sup> See *id.* at 4-148.

<sup>504</sup> See *id.*

<sup>505</sup> *Id.*

<sup>506</sup> See *id.* at 4-150 to -151.

<sup>507</sup> See *id.* at 4-155.

<sup>508</sup> See generally Sections IX.B. ("Insurance"); VIII.D. ("Notaries Public"), *infra*. Also, the possibility that the FCA may or should be placed within a "government corporation" is a repeated theme throughout this Report.

<sup>509</sup> See 40 U.S.C. § 757.

<sup>510</sup> *Id.* § 757(a)(1). This does not necessarily mean that the fund will not in the future get an appropriation with fiscal year limitation.

<sup>511</sup> See *id.*

<sup>512</sup> *Id.* § 757(b)(2).

### 3. Liability of the Federal Government Generally

Pursuant to the doctrine of sovereign immunity, the federal government is liable only to the extent it so consents;<sup>513</sup> exceptions to sovereign immunity are a matter of congressional consent or waiver.<sup>514</sup> Congress has granted such exceptions in a variety of areas.<sup>515</sup> If the government has a direct or indirect hand in running the FCA, it could face liability under the following statutes: the Federal Tort Claims Act (the "FTCA");<sup>516</sup> the Tucker Act<sup>517</sup> section 702 of the Administrative Procedure Act (the "APA");<sup>518</sup> and the Privacy Act.<sup>519</sup> The following discussion will assess the potential liability of the federal government as a provider of FCA services under each of these statutory provisions.

It should be noted that the governmental trend has been to move away from an original state of near total immunity towards increasing levels of liability exposure.<sup>520</sup>

---

<sup>513</sup> See *Kawananakoa v. Polyblank*, 205 U.S. 349 (1907).

<sup>514</sup> See, e.g., *Block v. North Dakota*, 461 U.S. 273, 280 (1983) ("The States of the Union, like *all other entities*, are barred by federal sovereign immunity from suing the United States in the absence of an express waiver of this immunity by Congress.") (emphasis added).

<sup>515</sup> See generally 14 C. WRIGHT, A. MILLER & E. COOPER, *FEDERAL PRACTICE AND PROCEDURE, JURISDICTION* 2D §§ 54-3660 (1985 & Supp. 1993). Section 3656 of the foregoing work, in particular, enumerates the various areas in which Congress has abrogated sovereign immunity.

<sup>516</sup> 28 U.S.C. §§ 1346(b), 2671-2680 (1988 & Supp. III 1991).

<sup>517</sup> 28 U.S.C. §§ 1346(a)(2), 1491. The Tucker Act deals, *inter alia*, with contract claims against the United States.

<sup>518</sup> 5 U.S.C. § 702.

<sup>519</sup> 5 U.S.C. § 552a.

<sup>520</sup> A sense of sovereign immunity's "big picture" appears in the following:

The shift from immunity has prompted a number of debates, in which the principal issues have been whether the immunity should be abolished, and if so whether by courts or legislatures; whether, if abolished by courts, it should be prospectively or retrospectively abolished; and whether the reform in immunity law can be achieved within a stable framework of law. To a large extent it appears that the



### a. Federal Tort Claims Act

With certain significant exceptions, the FTCA waives the federal government's sovereign immunity for actions in tort:

The United States shall be liable, respecting the provisions of this title relating to tort claims, in the same manner and to the same extent as a private individual under like circumstances, but shall not be liable for interest prior to judgment or for punitive damages.<sup>521</sup>

Courts have held that the FTCA's waiver of sovereign immunity is to be construed both strictly<sup>522</sup> and broadly.<sup>523</sup> Federal liability pursuant to the FTCA is "determined by the law of the place of the tort."<sup>524</sup> More specifically, "[s]uch liability for the acts or omissions of a civilian or military federal employee is determined by the law of *respondeat superior* of the state in which the act or omission occurred."<sup>525</sup> Two significant limitations on the general applicability of state law in FTCA actions, however, are that punitive damages are not available<sup>526</sup> and that the FTCA prohibits the imposition of liability without fault.<sup>527</sup>

---

change will continue, and the day may be at hand when the immunity as traditionally known no longer represents the first line of defense for governmental units.

PROSSER, *supra* note 197, § 131, at 1055-56.

<sup>521</sup> 28 U.S.C. § 2674.

<sup>522</sup> See, e.g., *Pennsylvania v. National Ass'n of Flood Insurers*, 520 F.2d 11, 19-20 (3d Cir. 1975).

<sup>523</sup> See, e.g., *Lozado v. United States*, 974 F.2d 986, 988 (8th Cir. 1992).

<sup>524</sup> *Garber v. United States*, 578 F.2d 414, 415 (D.C. Cir. 1978).

<sup>525</sup> *McSwain v. United States*, 422 F.2d 1086, 1088 (3d Cir. 1970) (citing *Williams v. United States*, 350 U.S. 857 (1955)); see Section IX.D.2., *infra* (presenting variant choice of law rules, Article 1, draft UNICTRAL Statutory Provisions).

<sup>526</sup> 28 U.S.C. § 2674.

<sup>527</sup> See *Laird v. Nelms*, 406 U.S. 797 (1972); *Dalehite v. United States*, 346 U.S. 15 (1953).

Thus, negligent operation of the FCA constituting the proximate cause of injury under state law would, in the absence of an applicable exception, give rise to a claim cognizable under the FTCA. Lost profits, if properly proven and not otherwise barred by a contractual limitation on liability, are recoverable.<sup>528</sup> Also relevant to the FCA is the potential under the FTCA for tortious invasion of privacy. Courts have recognized that the FTCA encompasses such a cause of action<sup>529</sup> but, in light of the fact that the FTCA creates no cause of action for violation or negligent observance of federal law,<sup>530</sup> have demanded that plaintiffs demonstrate a violation of state law. Thus, in *Zeller v. United States*, the court dismissed plaintiff's count under the FTCA in the following words:

[E]ven though the obligations and duties created by the Privacy Act bind federal agencies and their employees, see 5 U.S.C. § 552a, there is no law in New York placing upon private persons duties of non-disclosure such as those that the Privacy Act cast upon federal agencies.<sup>531</sup>

Federal liability under the FTCA is subject to a series of enumerated exceptions. Most relevant are the following:

(a) Any claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation, whether or not such statute or regulation be valid, or based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused.

(b) Any claim arising out of the loss, miscarriage, or negligent transmission of letters or postal matter. . . .<sup>532</sup>

(h) Any claim arising out of assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights. . . .

---

<sup>528</sup> See *Peck Iron and Metal Co., Inc. v. U.S.*, 603 F.2d 171 (Ct. Cl. 1979); *United States v. Griffith, Garnall & Carman, Inc.*, 210 F.2d 11 (10th Cir. 1954).

<sup>529</sup> See *Johnson v. Sawyer*, 760 F. Supp. 1216 (S.D. Tex. 1991); *Cruikshank v. United States*, 467 F. Supp. 539 (D. Haw. 1979).

<sup>530</sup> See *Feres v. United States*, 340 U.S. 135, 141-42 (1950).

<sup>531</sup> 467 F. Supp. 487, 505 (E.D.N.Y. 1979).

<sup>532</sup> The so-called "postal matter" exception is discussed at Section VII.A.4.a., *infra*.



(i) Any claim for damages caused by the fiscal operations of the Treasury or by the regulation of the monetary system. . . .<sup>533</sup>

### Discretionary Function Exemption

Section 2680(a) provides an important exemption for the government against certain suits that might arise from the behavior of its employees. The first part of this exemption protects the government against "[a]ny claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation, whether or not such statute or regulation be valid."<sup>534</sup> The second part covers employee activities deemed a part of a "discretionary function or duty."<sup>535</sup>

A few examples will give an idea of how this test is usually applied. In general, if the federal official is authorized to weigh potentially conflicting considerations in arriving at a decision, such a decision will fall squarely within the discretionary function exemption of the FTCA.<sup>536</sup> For example, governmental procedures for supervising the planning and building of a bridge which collapsed were considered "planning," not "operational," and therefore fell within the exemption.<sup>537</sup> However, discretionary function immunity does not "justify the government's failure to warn of risks created by its discretionary decisions, or to supply information that will allow other governmental agents or citizens themselves to proceed with greater safety."<sup>538</sup> Yet, the National Weather Service's

---

<sup>533</sup> *Id.* § 2680. On banking regulation, see Section VIII.A., *infra*.

<sup>534</sup> 28 U.S.C. § 2680(a). If the government or the employee violates a safety standard, this would generally mean that due care had not been exercised and the immunity would be removed. See PROSSER, *supra* note 197, § 131, at 1042.

<sup>535</sup> 28 U.S.C. § 2680(a). Note, the use of this exemption requires prior approval from the Department of Justice.

<sup>536</sup> 28 U.S.C. 2680(a).

<sup>537</sup> *In re Silver Bridge Disaster Litig.*, 381 F. Supp. 931 (S.D.W.Va. 1974).

<sup>538</sup> *Payton v. United States*, 679 F.2d 475 (5th Cir. 1982); *Emch v. United States*, 630 F.2d 523 (7th Cir. 1980) (allegation that federal agencies were negligent in permitting issuance of fraudulent and misleading reports to stockholders, in permitting fraudulent activities by officers and business associates of bank and of bank holding company, and in committing numerous mistakes, errors and omissions in course of examining bank and its holding company fell facially within discretionary function); *Kolb v. Naylor*, 658 F. Supp. 520 (N.D. Iowa 1987) (claim that the Federal Reserve Board . . . manipulated interest rates and thereby

failure to issue a warning regarding certain weather conditions has been considered discretionary.<sup>539</sup>

In its dealings with the public, it is unclear whether the FCA's activities would fall within the discretionary function exemption. On the one hand, issuance of certificates might appear to necessitate the exercise of discretion in deciding whether to accept certain CRD as the basis thereof. On the other hand, the acceptability of various forms of CRD may be regulated in the same manner as that supporting the issuance of passports,<sup>540</sup> in which case discretion would be altogether removed.<sup>541</sup> Remaining FCA functions, apart from those concerning CRLs, appear principally passive in nature, and CRL functions are contemplated to be undertaken upon user request or upon other contingencies that may also be regulated.

In general, application of the discretionary function requires "acts that involv[e] an element of judgment or choice."<sup>542</sup> Further, "[t]he requirement of judgment or choice is not satisfied if a 'federal statute, regulation, or policy specifically prescribes a course of action for an employee to follow.'"<sup>543</sup> However, absent a prescribed course of action, "it must be presumed that the agent's acts are grounded in policy when exercising . . . discretion."<sup>544</sup> Thus, ironically, the more strictly regulated an agent's actions, the more likely it is for the federal government to face liability. It would accordingly be possible for the FCA to shield itself from liability by promulgating a regulation along the lines of, "A certificate

---

brought about farm foreclosures). *But cf.* *Smith v. Johns-Manville Corp.*, 795 F.2d 301 (3d Cir. 1986) (failure of government to attach warning labels to asbestos it sold was held discretionary); *Begay v. U.S.*, 768 F.2d 1059 (9th Cir. 1985) (failure to warn of radiation exposure dangers held discretionary); *Barnson v. United States*, 816 F.2d 549 (10th Cir. 1987, *cert. denied*, 484 U.S. 896 (1987) (decision to warn entirely in agency's discretion).

<sup>539</sup> See *National Mfg. Co. v. United States*, 210 F.2d 263 (8th Cir.), *cert. denied*, 347 U.S. 967 (1954).

<sup>540</sup> See Section VIII.F., *infra*.

<sup>541</sup> Whether the activity is a government or proprietary function should also be considered.

<sup>542</sup> *Berkowitz v. United States*, 486 U.S. 531, 536 (1988).

<sup>543</sup> *United States v. Gaubert*, 499 U.S. 315 (1991) (quoting *Berkowitz*, 486 U.S. at 536).

<sup>544</sup> *Id.* at 316.



shall be issued upon presentation of such identification as may be deemed appropriate under the circumstances." However, such a regulation would effectively destroy the basis for legal presumptions<sup>545</sup> and the like deemed essential for the establishment of a useful FCA infrastructure. Hence, regulations will need to be issued, and the discretionary function exception will not likely be applicable.

### **Actions for Fraud, Deceit, and Misrepresentation**

Actions for fraud, deceit, and misrepresentation<sup>546</sup> are specifically excluded from the FTCA's scope pursuant to section 2680(h).<sup>547</sup> Even if a claim purports to be grounded in theories other than misrepresentation, the exception set out in 28 U.S.C. § 2680(h) would bar the action if deceit or misrepresentation were a factor relied upon to maintain a suit.<sup>548</sup> The *Silver Bridge Disaster*<sup>549</sup> case provides a

---

<sup>545</sup> Presumptions are explained and considered in LINKING SECURITY, *supra* note 2, § IV., at 59-67 and are subject to debate within the electronic commerce community.

These presumptions of law are based upon hypothesis. I refuse to hypothesize that computers cannot err. That plaintiff-appellant was presumed to have received this [insurance] premium notice, was surely a rebuttable presumption. . . . By a wisp of mental process, these presumptions of law are created. . . . A presumption is just like that: It is like a night bird, that flits about in the twilight and into the dark, but disappears under the light and sunshine of actual facts. The sunshine of the facts probe and reveal more than a presumption of law; we must never lose sight of this.

*Hughes Aircraft Co. v. United States*, 1993 WL 333379 (FED.CL.) (Aug. 16, 1993) (opinion on liability).

<sup>546</sup> "Any claim arising out of assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights. . . ." 28 U.S.C. § 2680(h).

<sup>547</sup> See, e.g., *Tapia v. United States*, 338 F.2d 416 (2d Cir. 1964), *cert. denied*, 380 U.S. 957 (1965); *United States v. Croft - Mullins Elec. Co.*, 333 U.S. 772 (5th Cir. 1964), *cert. denied*, 379 U.S. 968 (1965); *Goodman v. United States*, 324 F. Supp. 167 (M.D. Fla. 1971); *United States v. Gill*, 156 F. Supp. 955 (W.D. Pa. 1957).

<sup>548</sup> See *Kilduff v. United States*, 248 F. Supp. 310 (E.D. Va. 1960).

<sup>549</sup> See note 537, *supra*.

dramatic example of this exemption. Even though a survey published under the name of the federal government asserted that the bridge was capable of a certain loading and reliance on that information led to the deaths of motorists when the bridge collapsed, the claim was barred under the FTCA because it depended on the government's misrepresentation of the bridge's safety.<sup>550</sup>

FCA activities, improperly performed, could give rise to a number of causes of action falling within the section 2680(h) exception for misrepresentation or interference with contractual relations. Indeed, because this Report conceives of the making of "representations" (or "certifications") probably as the FCA's primary function, the section 2860(h) exception for liability in tort could conceivably curtail much potential liability, even to the point where it is diminished to an undesirable degree. The issuance of a certificate to a fraudster, for example, could conceivably give rise to a claim of misrepresentation on the part of the FCA because of false CRD. Moreover, section 2680(h) applies to claims for both *negligent* and *intentional* misrepresentation.<sup>551</sup> Finally, failure to issue a certificate or, more probably, wrongful issuance of a CRL, could easily be construed as an interference with contractual relations. These claims would be barred.

### Liability of Federal Employees

Provided they are acting within the scope of their duties, federal employees are absolved of liability in tort by section 2679, which provides, with certain exceptions, that a plaintiff's exclusive remedy for tortious activity on behalf of the United States is that provided against the United States by the FTCA<sup>552</sup> and that actions against employees who have been certified by the Attorney General to have been acting within the scope of employment are deemed to be against the United States alone, subject to judicial review.<sup>553</sup> However, given that liability

---

<sup>550</sup> See *In re Silver Bridge Disaster Litig.*, 381 F. Supp. 931 (S.D.W.Va. 1974).

<sup>551</sup> *United States v. Newstadt*, 366 U.S. 696 (1961).

<sup>552</sup> See 28 U.S.C. § 2679(b)(1).

<sup>553</sup> See *id.* 2679(d)(1). The principal exception to this treatment is for so-called *Bivens* actions. In *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971), the Supreme Court implied a right of action against individual agents for violating plaintiff's Fourth Amendment rights. Federal law now preserves this right as an exception to the general exclusivity rule of section 2679(b)(1). See 28 U.S.C. § 2679(b)(2). See *Pereira v. U.S. Postal Service*, 964 F.2d 873, 876 (9th Cir. 1992)



under the FTCA is predicated upon principles of *respondeat superior*, the government is *not* financially responsible for torts committed by federal employees acting outside the scope of their employment.<sup>554</sup>

### Liability of the Federal Government for Acts of Private Contractors

The liability of the federal government for the acts of independent contractors is conceptually unproblematic: "As used in [the FTCA], the term 'Federal agency . . . does not include any contractor with the United States.'"<sup>555</sup> Accordingly, the federal government has simply not waived sovereign immunity for the acts of independent contractors. However, substance prevails over form in this area as well as in the analogous one under the Tax Code, and merely calling an entity performing services an "independent contractor" is not determinative. Thus, "a critical element of distinguishing an agency from a contractor is the power of the Federal Government to control the detailed physical performance of the contractor."<sup>556</sup> Moreover, the federal government may face liability for negligence in contracting, both in terms of substantive provisions<sup>557</sup> and in terms of the contractor selected.<sup>558</sup>

---

(join[ing] a parade of other circuits in precluding the use of *Bivens* actions to supplement Congress' remedial scheme[s].").

<sup>554</sup> See 28 U.S.C. § 1346(b) (limiting federal jurisdiction over tort claims against the United States to those caused by federal employees acting within the scope of employment). Acting within the scope of one's duties is, of course, a predicate for an employer's liability under a theory of *respondeat superior*. See RESTATEMENT (SECOND) OF TORTS § 877.

<sup>555</sup> 28 U.S.C. § 2671.

<sup>556</sup> See, e.g., *United States v. Orleans*, 425 U.S. 807, 814 (1976); see also *Logue v. United States*, 412 U.S. 512 (1973); *Bird v. United States*, 949 F.2d 1079 (10th Cir. 1991); *Leone v. United States*, 910 F.2d 46 (2d Cir. 1990), *cert. denied*, 499 U.S. 905 (1991); *Bowman v. U.S.* 821 F. Supp. 1442 (D. Wyo. 1993).

<sup>557</sup> See, e.g., *Phillips v. United States*, 956 F.2d 1071 (11th Cir. 1992).

<sup>558</sup> See, e.g., *New York v. Shore Realty Corp.*, 648 F. Supp. 255 (E.D.N.Y. 1986). See also *United States v. Orleans*, 425 U.S. 807 (1991) (receipt of federal funds and obligation to comply with federal standards not controlling).

## b. The Tucker Act

The Tucker Act provides the "exclusive basis for asserting contract claims against the United States."<sup>559</sup> The Act provides, in relevant part, that "[t]he United States Court of Federal Claims shall have jurisdiction to render judgment upon any claim against the United States founded . . . upon any express or implied contract with the United States, or for liquidated or unliquidated damages in cases not sounding in tort."<sup>560</sup>

The issuance of a certificate by the FCA might be considered as giving rise to an express or implied contractual obligation for the appropriate provision of FCA services, especially if, for example, a fee were charged at the time of the certificate's issuance or from time to time over the period during which the certificate remains in effect. In the absence of a fee or other consideration, it is conceivable that a quasi-contractual relationship might arise under a theory of promissory estoppel or the like. However, the courts have repeatedly held that the Tucker Act does not confer jurisdiction over contracts implied at law.<sup>561</sup>

Although the vast majority of the Tucker Act cases concern government employment and procurement contracts, the statute has been applied to other sorts of contracts as well. These contracts need not be "formal" and may arise in unexpected circumstances. Thus, in *Hatzlachh*,<sup>562</sup> the Supreme Court, over the dissent of Justice Blackmun, remanded on the issue of the existence of a contract implied in fact between the United States Customs Service and the importer-petitioner for the intact return of seized goods after payment of a penalty.<sup>563</sup>

---

<sup>559</sup> *Metadure v. United States*, 490 F. Supp. 1368, 1371 (S.D.N.Y. 1980) (citing *Polos v. United States*, 556 F.2d 903, 905 (8th Cir. 1977); *International Eng'g Co. v. Richardson*, 512 F.2d 573 (D.C. Cir. 1975), *cert. denied*, 423 U.S. 1048 (1976)).

<sup>560</sup> 28 U.S.C. § 1491(a). Section 1346(a)(2), sometimes referred to as the "Little Tucker Act," vests similar and concurrent jurisdiction in the federal district courts for claims not exceeding \$10,000 in amount. 28 U.S.C. § 1346(a)(2).

<sup>561</sup> See, e.g., *Hatzlachh Supply Co., Inc. v. United States*, 444 U.S. 460, 465 n.5 (1980) (dicta); *GAF Corp. v. United States*, 932 F.2d 947, 951 (Fed. Cir. 1991), *cert. denied*, \_\_\_ U.S. \_\_\_, 112 S. Ct. 965 (1992); *Atlas Corp. v. United States*, 895 F.2d 745, 755 (Fed. Cir.), *cert. denied*, 498 U.S. 811 (1990).

<sup>562</sup> 444 U.S. 460 (1980).

<sup>563</sup> Justice Blackmun was "persuaded that an implied-in-fact contract is not to be found on the record" because the Customs Service had a pre-existing legal duty to return the goods if their seizure were determined to have been unwarranted. *Id.* at 467 (Blackmun, J., dissenting).



Although the United States Claims Court later determined on the facts that no such contract had come into existence,<sup>564</sup> *Hatzlachh* demonstrates the clear potential for the government to find itself a viable defendant in perhaps unexpected circumstances.

Authority regarding the contractual liability of the government for compensated services rendered is meager. There is authority for the proposition that contractual liability under the Tucker Act is limited to situations in which governmental services are performed on a discretionary basis. In *Heil v. United States*,<sup>565</sup> Judge Learned Hand overruled the United States' demurrer to an action in contract brought by the plaintiff for failure to transmit a telegraph message while the telegraph systems were under federal control during World War I.<sup>566</sup> In holding that the United States had subjected itself to contractual liability for operating the telegraph system, the court made the following distinction:

... Congress meant to assume liability [under the Tucker Act] for the acts of such of its agents as had the power in the discharge of their duties to assume or refuse engagements on the faith of which other citizens should rely. It did not mean to assume liability for the proper discharge of duties which it imposed upon those agents by virtue only of positive law.<sup>567</sup>

The clear, if inexplicable implication is that the Tucker Act would have afforded no remedy if the government had chosen to operate the telegram system as a "common carrier," "under compulsion to serve all comers."<sup>568</sup> In terms of this distinction, federal liability under *Heil* is the polar opposite of the "discretionary function" exception to liability under the FTCA.<sup>569</sup> Finally, *Heil* remains "good

---

<sup>564</sup> *Hatzlachh v. United States*, 7 Cl. Ct. 743 (1985).

<sup>565</sup> 273 F. 729 (S.D.N.Y. 1921).

<sup>566</sup> Although the court did not mention the issue, it is interesting to note that the plaintiff was seeking consequential damages: "the message was for the purchase of £100,000 sterling, and the loss depended upon fluctuations in British exchange." *Id.* at 730.

<sup>567</sup> *Id.* at 731.

<sup>568</sup> See text accompanying note 234, *supra*; see also Section VIII.G., *infra* ("Common Carriers").

<sup>569</sup> See 28 U.S.C. § 2680(a); see text accompanying notes 565 and 567, *supra*. It should be noted that *Heil* was decided long before the 1946 enactment of the FTCA. It is also interesting to note that telegraph operations during World War I

law": its reasoning has never been brought into question,<sup>570</sup> and its distinction has been followed<sup>571</sup> but never explicated.

Tucker Act claimants have also had success in asserting causes against the government for breach of the contract of bailment.<sup>572</sup> In the most famous of these cases, the plaintiff succeeded in its action for breach of a contract of bailment when a quantity of goods mysteriously disappeared overnight during the customs inspection process. The court held, "The obligation of the government was not artificially created by law but rather stemmed from an implied promise to redeliver the goods as soon as customs had checked them against the invoice."<sup>573</sup> Moreover, the *Alliance Assurance* court specifically held that no consideration beyond the act of entrustment was necessary to bind the government.<sup>574</sup>

Given the fact that users will be required as a practical matter to entrust valuable information to the FCA, bailment cases under the Tucker Act are of clear relevance to the present inquiry. The foregoing authorities establish that the potential for federal liability under the Tucker Act in respect of the FCA is

---

were conducted under the authority of the Postmaster General. *See Heil*, 273 F. at 731.

<sup>570</sup> The Supreme Court has expressly refused to consider the correctness of *Heil's* result. *See Western Union Tele. Co. v. Porton*, 256 U.S. 662, 667 n.2 (1921) (private telegraph company may not be held liable for government's acts and omissions during period of federal operation).

<sup>571</sup> *See, e.g., Nickola v. United States*, 137 F. Supp. 943, 944 (E.D. Mich. 1956) (limiting Postal Service's liability in contract to that expressed in "statutes and postal regulations"; *Heil* provides alternative ground for dismissing complaint).

<sup>572</sup> *See, e.g., Alliance Assurance Co., Ltd. v. United States*, 252 F.2d 529 (2d Cir. 1958); *C.F. Harms Co. v. Erie R.R. Co.*, 167 F.2d 562 (2d Cir. 1948) (damage to vessel commandeered by U.S. Army during World War II); *Price v. United States*, 707 F. Supp. 1465 (S.D. Tex. 1989) (failure to return film archives and water-color paintings by Adolph Hitler seized from Nazi Germany). *See also* Section VIII.C.3. ("Bailor - Bailee Relationship"), *infra*.

<sup>573</sup> *Alliance Assurance*, 252 F.2d at 532.

<sup>574</sup> *See id.* at 533 (quoting, *inter alia*, *Coggs v. Bernard*, 2 Reym. 909, 919, 92 Eng. Rep. 107, 113 (1703)). The fact that the "bailment" in *Alliance Assurance* was compulsory was a separate but "more compelling reason to find consideration exists." *Id.* On the law of bailments generally, *see* Section VIII.C.3., *infra*.



substantial, particularly if the FCA attempts to take advantage of the "discretionary function" exception to the FTCA.

### c. The Administrative Procedure Act

Section 702 of the APA constitutes an additional, limited, waiver of sovereign immunity:

A person suffering legal wrong because of agency action . . . is entitled to judicial review thereof. An action in a court of the United States seeking relief other than monetary damages and stating a claim that an agency or an officer or employee thereof acted or failed to act in an official capacity or under color of legal authority shall not be dismissed nor relief therein be denied on the ground that it is against the United States . . .<sup>575</sup>

Three important limitations on jurisdiction over section 702 claims exist: "the APA excludes from its waiver of sovereign immunity (1) claims for money damages, (2) claims for which an adequate remedy is available elsewhere, and (3) claims seeking relief expressly or implicitly forbidden by another statute."<sup>576</sup> Under the latter two limitations, tort and contract actions would ordinarily be permitted or prohibited by the FTCA and the Tucker Act, respectively, thus precluding relief under the APA in either case.<sup>577</sup> However, the Supreme Court has recently denied these concepts talismanic value by holding that the ostensibly "contractual" claims of a state under the Medicaid program are not uniquely remediable by an action for damages: "We are not willing to assume, categorically, that a naked money judgment against the United States will always be an

---

<sup>575</sup> 5 U.S.C. § 702.

<sup>576</sup> *Transohio Sav. Bank v. Director*, 967 F.2d 598, 607 (D.C. Cir. 1992); *accord*, *Smith v. Washington Heights Apartments, Ltd.*, 794 F. Supp. 1141, 1143 (S.D. Fla 1992). These limitations derive from sections 702 ("An action . . . seeking relief other than monetary damages . . . shall not be dismissed . . ."; "Nothing herein . . . confers authority to grant relief if any other statute that grants consent to suit expressly or implicitly forbids the relief which is sought") and 704 ("Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review"). 5 U.S.C. §§ 702, 704; *see also* 5 U.S.C. § 701(a)(1) (denying availability of section 702 actions when "statutes preclude judicial review").

<sup>577</sup> *See, e.g., Transohio*, 967 F.2d at 608-613 (Tucker Act provides exclusive remedy for contract actions for damages, but does not confer jurisdiction over contract actions seeking equitable relief; claims arising out of statutory and constitutional violations cognizable under section 702).

adequate substitute for prospective relief fashioned in the light of the rather complex ongoing relationship between the parties."<sup>578</sup> Moreover, although section 702 does not permit actions for monetary *damages*, courts may grant monetary *relief* pursuant to it.<sup>579</sup>

A final limitation on judicial review of agency action pursuant to the APA is when "agency action is committed to the agency's discretion by law."<sup>580</sup> This exception to section 702 is "narrow" and essentially applies only when "statutes are drawn in such broad terms that in a given case there is no law to apply"<sup>581</sup> for purposes of judicial review.

Although it is likely that most, if not all, actions against the United States in respect of the FCA would be for "damages" and would accordingly be governed by the FTCA, the Tucker Act, or any statutes and/or regulations establishing the FCA, the possibility for monetary relief under section 702 is deserving of note, particularly when the FCA's nature remains amorphous.

---

<sup>578</sup> *Bowen v. Massachusetts*, 987 U.S. 879, 905 (1988).

<sup>579</sup> *See id.* at 892-901 (retroactive declaratory and injunctive relief requiring the payment of sums owing in challenge to determination that certain medical expenses were not reimbursable under Medicaid program); *see also* *De Vargas v. Mason & Hanger-Silas Mason Co., Inc.*, 911 F.2d 1377, 1381 n.3 (10th Cir. 1990), *cert. denied*, 298 U.S. 1074 (1991).

<sup>580</sup> 5 U.S.C. § 701(a)(2).

<sup>581</sup> *Citizens To Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 902, 910 (1971) (quoting S. Rep. No. 752, 79th Cong., 1st Sess. 26 (1946)); *see also*, *Haitian Refugee Ctr., Inc. v. Baker*, 953 F.2d 1498, 1507 (11th Cir.), *cert. denied*, \_\_ U.S. \_\_, 112 S.Ct. 1245 (1992); *International Union v. Donovan*, 746 F.2d 855, 863 (D.C. Cir. 1984), *cert. denied*, 474 U.S. 825 (1985).



#### d. Privacy Act

While not generally a separate source of federal liability, the Privacy Act<sup>582</sup> constitutes a relatively comprehensive set of rules for the handling by the government of information respecting "individuals"<sup>583</sup> which may directly or by analogy govern the FCA. It should be noted in the section below concerning federal contractors<sup>584</sup> that

When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of the section to be applied to such system. For purposes of subsection (i) of this section . . . any such contractor and any employee of such contractor . . . shall be considered to be an employee of an agency.<sup>585</sup>

The Privacy Act focuses upon two fundamental concerns: the integrity of "records"<sup>586</sup> compiled by federal agencies, and the limitation or prohibition on their *disclosure*. Congress amended the Privacy Act in 1988<sup>587</sup> to institute statutory protections for individuals, in the context of computerized "matching" of data.<sup>588</sup>

---

<sup>582</sup> 5 U.S.C. § 552a.

<sup>583</sup> "Individual" is defined to mean "a citizen of the United States or an alien lawfully admitted for permanent residence." *Id.* § 555a(a)(2).

<sup>584</sup> See Section VII.B. ("The Federal Government as Contractor for FCA Services"), *infra*.

<sup>585</sup> 5 U.S.C. § 552a(m)(c).

<sup>586</sup> A "record" is:

. . . any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph . . .

*Id.* § 552a(a)(4). ("Records maintained on individuals").

<sup>587</sup> Pub. L. No. 100-503, § 2, 102 Stat. 2507 (1988).

<sup>588</sup> The Internal Revenue Service, for example, has frequently agreed with various States to match income tax return data.

With respect to data integrity, the Privacy Act imposes a lengthy list of requirements, including that "records" be "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";<sup>589</sup> that "policies and procedures of the agency regarding storage, retrievability, access controls, retention, and disposal" be published in the Federal Register;<sup>590</sup> that "records which are used by the agency in making any determination about any individual be maintained";<sup>591</sup> that "no record describing how any individual exercises rights guaranteed by the First Amendment [unless otherwise authorized by statute or by the individual, or in the course of law enforcement activities]" be maintained;<sup>592</sup> that each agency establish "rules of conduct: for its employees";<sup>593</sup> that each agency "insure [sic] the security and confidentiality of records and to protect against any anticipated threats or hazards to their security and integrity";<sup>594</sup> that each agency "establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him";<sup>595</sup> and that each agency "define reasonable times, places, and requirements for identifying an individual . . . before the agency shall make the record available [to him]."<sup>596</sup> All of these concerns are relevant to the FCA and to other issues discussed herein.

Subsection 552a(d) permits an individual to inspect records pertaining to him, request amendment and dispute adverse determinations.<sup>597</sup> The right of inspection, however, does not extend to "information compiled in reasonable anticipation of a civil act or proceeding."<sup>598</sup>

---

<sup>589</sup> 5 U.S.C. § 552(e)(1).

<sup>590</sup> *Id.* § 552(e)(4)(e).

<sup>591</sup> *Id.* § 552(e)(5).

<sup>592</sup> *Id.* § 552(e)(7).

<sup>593</sup> *Id.* § 552(e)(9).

<sup>594</sup> *Id.* § 552(e)(10).

<sup>595</sup> *Id.* § 552a(f)(1).

<sup>596</sup> *Id.* § 552a(2).

<sup>597</sup> *Id.* § 552a(d).

<sup>598</sup> *Id.* § 552a(d)(5).



However, certain agencies, including the Central Intelligence Agency and those involved in the enforcement of criminal laws, may exempt their records from many (but by no means all) of the foregoing.<sup>599</sup> Any agency may also exempt records even more broadly if, *inter alia*, they concern the national defense,<sup>600</sup> law enforcement,<sup>601</sup> or "testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal Service."<sup>602</sup>

The Privacy Act prohibits agencies from disclosing an individual's records absent request or written consent from the subject of those records other than pursuant

---

<sup>599</sup> *Id.* § 552a(j).

<sup>600</sup> *See id.* § 552a(k)(i) (incorporating by reference § 552(b)(1), which exempts such records from the scope of the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(b)(1)).

<sup>601</sup> *See id.* § 552a(k)(2).

<sup>602</sup> *Id.* § 552a(k)(6).

to FOIA<sup>603</sup> "routine use,"<sup>604</sup> and for law enforcement purposes,<sup>605</sup> among other things. Agencies must reveal to individuals the disclosure of records relating to them in a variety of circumstances. However, agencies may exclude their records from the scope of the foregoing disclosure and accounting rules for many of the same reasons and in the same circumstances as is the case with the "integrity" rules set forth above.<sup>606</sup>

The "matching" legislation of 1988<sup>607</sup> in reality forms part of the "anti-disclosure" focus of the Privacy Act. A "matching program" is a computerized comparison of two or more automated federal personnel record systems or two or more automated record systems (at least one of which is maintained by a federal agency) when the comparison is made to establish or verify eligibility for a compliance

---

<sup>603</sup> See *id.* § 552a(b)(2).

FOIA establishes a comprehensive scheme for citizens to obtain access to agency records. See *id.* § 552(a)(3). Of relevance to the FCA are the following limitations or exclusions:

1. "To the extent required to prevent a clearly unwarranted invasion of privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement or policy, interpretation, or staff manual or instruction," *id.* § 552(a)(2);
2. matters that are related to the national defense, see *id.* § 552(b)(1);
3. matters specifically exempted from disclosure by statute (with the exception of the Privacy Act), see *id.* § 522(b)(3);
4. constitute trade secrets and commercial or financial information obtained from a person and privileged and confidential, see *id.* § 522(b)(4);
5. constitute personnel and medical files and similar files the disclosure of which would be an unwarranted invasion of privacy, see *id.* § 522(b)(6) and
6. related to law enforcement, see *id.* § 522(b)(7) or certain banking matters, see *id.* § 522(b)(8).

<sup>604</sup> *Id.* § 522(b)(3). "[R]outine use means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7).

<sup>605</sup> *Id.* § 552a(b)(7).

<sup>606</sup> See notes 589 - 596, *supra*, and accompanying text.

<sup>607</sup> See note 588, *supra*.



with federal benefit programs.<sup>608</sup> Excluded from the definition of "matching program" are matches made for purposes of statistical analysis, law enforcement, taxation, routine federal personnel administration and security clearance.<sup>609</sup>

Matching programs must be performed pursuant to written agreements containing a large number of protective provisions,<sup>610</sup> and action adverse to an individual or the basis thereof is subject to verification processes and rights on the part of individuals to contest findings.<sup>611</sup> The legislation directs agencies to establish "Data Integrity Boards" to oversee compliance with the matching program's protective provisions.<sup>612</sup>

Individuals may bring civil actions for injunctive relief and/or money damages plus attorney's fees and costs against agencies for their failure to comply with the Privacy Act.<sup>613</sup> Moreover, criminal penalties may apply against agency officers and employees for their willful violations of the Privacy Act.<sup>614</sup>

Finally, section 552a has a "metaphorical" dimension which has embodied in relatively compact form many of the central informational privacy concerns of any FCA debate and/or implementation. One need not be pleased with the controversial policy decisions that underpin the entire structure in order to acknowledge that, to some degree, all future informational privacy debates will have many of its terms dictated by the Privacy Act.

#### **4. Notable FCA Candidates**

##### **a. United States Postal Service**

The United States Postal Service (the "USPS" or the "Postal Service") is a potential candidate for FCA functions because of its history of providing extensive

---

<sup>608</sup> See 5 U.S.C. § 552a(a)(8).

<sup>609</sup> See *id.* § 552a(a)(8)(B).

<sup>610</sup> See *id.* § 552a(o).

<sup>611</sup> See *id.* § 552(p).

<sup>612</sup> *Id.* § 552a(a).

<sup>613</sup> See *id.* § 552a(g).

<sup>614</sup> See *id.* § 552a(i).

public communication services its existing network of facilities. Also, the USPS has an established history of developing new methods of communication (e.g., telegraph and air mail) and an established tradition of offering graduated categories of mail service that permits customers to purchase various levels of delivery assurance.<sup>615</sup> Accordingly, this Report gives substantial consideration to USPS as a possible (or partial) home for FCA operations.

### Authority to Undertake FCA Operations

Not surprisingly, no provision of the Postal Reorganization Act of 1970 (the "PRA")<sup>616</sup> specifically addresses FCA administration. However, FCA administration may be within the broad scope of the Postal Service's purpose, and the Postal Service is specifically authorized to provide special nonpostal services which may be outside its traditional physical mail delivery functions. Section 404(a)(6) of Title 39 provides:

Without limitation of the generality of its powers, the Postal Service shall have the following specific powers, among others:

...

(6) to provide, establish, change, or abolish special nonpostal or similar services . . . .<sup>617</sup>

If administration of the FCA is a "nonpostal" activity, the question arises whether the Postal Service is authorized by statute to engage in such efforts. Agency actions

---

<sup>615</sup> See, e.g., USPS DOMESTIC MAIL MANUAL, Issue 42 (effective Mar. 15, 1992) Ch. 3 (concerning first-class mail); § 912 (concerning certified mail); § 911 ("The registered mail system provides added protection for valuable and important mail. Postal insurance coverage may be purchased for mail which is registered in case of loss or damage. Registered mail is the most secure service the Postal Service offers. It incorporates a system of receipts to monitor the mail's movement from the point of acceptance to delivery."); § 915 ("Special delivery mail is given preferential handling to the extent practical in dispatch and transportation."); Ch. 2 ("Express mail is a highly reliable expedited postal service, available with five basic service offerings.").

<sup>616</sup> Pub. L. No. 91-375, 84 Stat. 719 (1970), codified at 39 U.S.C. §§ 101 *et seq.*

<sup>617</sup> 39 U.S.C. § 404(a)(6). The absence of a comma between "special" and "nonpostal" appears to be an oversight. Courts have apparently read section 404(a)(6) to include a comma between "special" and "nonpostal." See, e.g., *Associated Third Class Mail Users v. U.S.P.S.*, 405 F. Supp. 1109, 1117 (D.D.C. 1975). On appeal, the court noted that "it is generally agreed that the absence of a comma between 'special' and 'nonpostal' was inadvertent." *National Ass'n of Greeting Card Publishers v. U.S.P.S.*, 569 F.2d 570, 597, n.1119 (D.C. Cir. 1976).



in excess of statutory authority are void, and there is no judicial or legislative support for reading section 404(a)(6) so broadly that it authorizes, without restraint, postal entry into any business. However, there are at least two reasons why administration of a FCA might be an appropriate "nonpostal" service for the Postal Service to undertake. First, the Postal Service has resources that make it uniquely fitted to this role. If the issuing of certificates to a broad population is one of the goals of the program, approximately 30,000 retail facilities provide the same type of resource currently used for Selective Service registration, passport applications, and other services.

Second, an important USPS asset relevant to the FCA is the Zip Code database. This massive relational database registers (for the purposes of post handling and other functions) residential and business localities as well as associated routing information required for the delivery and transfer of postal mail to Zip Code areas. The USPS also provides ancillary services such as postal mail forwarding in which individual subscribers are named and their forwarding and "leaving" addresses are registered. This information is provided exclusively via subscription service to the subject postal subscriber.

The Postal Zip Code database could benefit the FCA infrastructure because of its high quality source of national, state and locality components (of a X.500 Distinguished Name) that support consistent and accurate validation of names purporting to be based upon the actual civil naming infrastructure. In this regard, the USPS has demonstrated its capacity to manage and provide a residential and organizational naming and certificate directory.

Third, and more importantly, the proposed service may fit within the broad goals of postal policy. Section 101 of the PRA provides, in relevant part:

(a) The United States Postal Service shall be operated as a basic and fundamental service provided to the people by the Government of the United States, authorized by the Constitution, created by Act of Congress, and supported by the people. The Postal Service shall have as its basic function the obligation to provide postal services to bind the Nation together through the personal, educational, literary, and business correspondence of the people . . .<sup>618</sup>

These broad goals might be accomplished by means other than the physical delivery of hard-copy letters. There is language in the legislative history of the PRA that suggests such proposals should be viewed broadly:

The Postal Service is empowered to engage in research and development programs directed toward the expansion of present postal service and the development of new services responsive to the evolving needs of the United States.<sup>619</sup>

---

<sup>618</sup> 39 U.S.C. § 101(a).

<sup>619</sup> H.R. Rep. No. 1104, 91st Cong., 2d Sess. 9 (1970).

Administration of an FCA would appear, in this respect, to be consistent with Congress' intent to "[c]reate a lasting foundation of a modern, dynamic, and viable postal institution that is both equipped and empowered at all times to satisfy the postal requirements of the future technological, economic, cultural, and social growth of the Nation . . . ." <sup>620</sup> First, FCA functions support the "correspondence of the people" in that certification will foster the reliability and trustworthiness of electronic correspondence. Thus, if the USPS were to perform FCA functions, the recipient of a digitally signed electronic message might trust the authenticity of the digital signature it bears because of its certification by the (presumptively trustworthy) USPS.

Second, Congress provided that the USPS "shall provide prompt, reliable, and efficient services to patrons in all areas and shall render postal services to all communities. . . ." <sup>621</sup> The pervasive establishment of post offices would permit the USPS to perform certification (of, *e.g.*, individuals and small businesses) through its pre-existing (highly distributed) offices.

Third, Congress provided that "[i]n selecting modes of transportation, the Postal Service shall give highest consideration to the prompt and economical delivery of all mail" including "[m]odern methods of transporting mail by containerization and programs designed to achieve overnight [service]." <sup>622</sup> As electronic correspondence becomes a widely spread, "prompt and economical" form of correspondence, this mandate might provide sufficient authorization for the USPS to facilitate correspondence through FCA functions. However, the scope of section 101 has been the subject of minimal judicial attention, and whether or not it authorizes the USPS to perform FCA functions remains unclear.

Finally, the USPS has authority to develop new programs to improve the adequacy and efficiency of its business. <sup>623</sup> Courts have broadly construed these powers and have been unwilling to frustrate experimentation with innovative

---

<sup>620</sup> *Id.* at 2.

<sup>621</sup> *Id.*

<sup>622</sup> 39 U.S.C. § 101(f). Also, the USPS shall give "highest consideration to the requirement for the most expeditious collection, transportation and delivery of important letter mail." 39 U.S.C. § 101(e).

<sup>623</sup> 39 U.S.C. § 403(a) ("The postal service shall plan, develop, promote, and provide adequate and efficient postal services at fair and reasonable rates and fees"). Intriguingly, "postal services" is *not* a defined term.



techniques through implied restrictions upon its authority.<sup>624</sup> Accordingly, if the USPS were willing to undertake FCA functions, strong arguments can be made that the authority to do so exists under currently applicable law, at least on an experimental basis.

Interestingly, the Postal Service has been acknowledged as having a broader role in communications than the acceptance, transportation and delivery of physical mail. For example, over one hundred years ago, William Howard Taft, acting Attorney General, observed that:

It is manifest that the object of the establishment of postal facilities was the transmission of intelligence for the uses and benefit of the people at large. This purpose was primary and creative, and the methods of communication were subordinate and subject to opportunity and convenience.<sup>625</sup>

Although Taft decided that the Postal Office Department was without power to contract for telegraphic transmission of mail matter because Congress had failed to authorize the expenditure, he recognized that there was no inherent limitation on the power of the Post Office Department to engage in radically different kinds of communication.<sup>626</sup>

---

<sup>624</sup> See, e.g., *United Tele. Workers v. FCC*, 436 F.2d 920, 926 (D.C. Cir. 1970) (upholding the experimental provision of "Mailgram" services pursuant to which the USPS would mail communications telexed directly to its offices). The court, however, placed considerable emphasis on the *experimental* nature of the service. See *id.* at 926 (citing *Atchison, T & S.F. Ry. Co. v. Summerfield*, 128 F. Supp. 266 (D.D.C), *rev'd in part*, 229 F.2d 777 (D.C. Cir. 1955), *cert. denied*, 351 U.S. 926 (1956)). In *Atchison*, the court upheld an experiment in the carriage of mail by air, but held that it could not be "unduly prolonged." 128 F. Supp. at 274.

<sup>625</sup> 19 Op. Att'y. Gen. 650, 652 (1890).

<sup>626</sup> See *id.* at 655. In fact, he stated:

Thus, it appears that the comprehensive idea of "general transmission of intelligence" in connection with the post office, expressed in 1775, was, under the authority of Congress, applied to and employed in connection with the telegraph by the Post-Office Department in 1845-'46.

*Id.* at 652.

## Administration and Freedom from Political Influence

Under the PRA, Congress vested an eleven-member, independent, Board of Governors with exclusive authority to manage the postal service in order to plan, develop, and promote mail services.<sup>627</sup> Although nine of the Board of Governors are appointed by the President, a recent decision found that a district court could enjoin the President from removing members of the Board of Governors when the Court of Appeals had determined *de facto* that (1) it had jurisdiction over the subject matter of the dispute; (2) removal would jeopardize the court's jurisdiction; and (3) temporary postponement would cause no damage to the President's interest.<sup>628</sup>

Congress also created a separate Postal Rate Commission (the "PRC") as an "independent establishment of the executive branch . . . ." Its five members serve six year terms, and no more than three of them may be "adherents of the same political party."<sup>629</sup> The postal service is required to request a recommended decision from the PRC for making rate changes, fees or classifications. But, the PRC does not have direct authority to regulate the Postal Service.<sup>630</sup> The Act also

---

<sup>627</sup> See 39 U.S.C. § 202. The President appoints nine Governors to nine year terms with the advice and consent of the Senate. The Governors appoint the Postmaster General and the Deputy Postmaster General, who is appointed with the additional participation of the Postmaster General. No more than five of the Governors are to be "adherents of the same political party." *Id.* § 202(a), (b). Prior to enactment of the PRA management decisions were shared among eight different governmental agencies having jurisdiction over finance, transportation, and other functions. See Note, *The Postal Reorganization Act: A Case Study of Regulated Industry Reform*, 58 VA. L. REV. 1030, 1032 (1972). The managers had broad duties, but their powers were perceived as insufficient in scope for their proper performance. See, e.g., *U.S.P.S. Governors v. Postal Rate Comm'n*, 654 F.2d 108, 109 (D.C. Cir. 1981). Among the principal goals of the PRA was to reform this diffusion in management authority and to "free postal management from entangling red tape and to concentrate management authority so as to provide an efficient and economical postal system." *Id.*

<sup>628</sup> See *Mackie v. Bush*, 809 F. Supp. 144 (D.D.C. 1993). In a related case, the Court of Appeals found that the P.R.C. permits the Postal Service to seek judicial review on its own if the Department of Justice has declined to represent its fundamental positions or to consent to its self-representation. See *Mail Order Ass'n of Am. v. U.S.P.S.*, 986 F.2d 509 (D.C. Cir. 1993).

<sup>629</sup> 39 U.S.C. §§ 3601, 3602.

<sup>630</sup> See *id.* §§ 3622, 3623. After a Postal Service request for recommendations on rates and classifications, the PRC must provide the USPS and users of the mails



requires an advisory opinion from the PRC on changes "in the nature of postal services which will generally affect service on a nationwide or substantially nationwide basis."<sup>631</sup> Upon receiving a recommendation from the PRC, the Governors may either approve it and order it to take effect, reject it, or modify it (the Governors may only modify a recommended decision upon the unanimous written concurrence of all governors pursuant to 39 U.S.C. § 3625(d)). The PRC is not authorized to overrule or modify a decision by the Board of Governors.<sup>632</sup>

### Politics of Situating the FCA Within the USPS

Despite statutory initiatives to the contrary, the USPS is not immune from political pressures, and placement of the FCA within the USPS would require the negotiation of delicate political territory. Several factors can limit the Postal Service's political independence.<sup>633</sup> First, although the vast majority of postal funds are obtained from postal rate payers, the Postal Service can be subject to the vagaries of the annual appropriations process and its budgets have been threatened by appropriations bill riders. Several House and Senate committees

---

an opportunity for a hearing under the Administrative Procedure Act, *See* 5 U.S.C. §§ 556-557; 39 U.S.C. § 3624a. The recommended decision must address specific statutory criteria appearing in sections 3622 and 3623. *See* 39 U.S.C. § 3624(d).

<sup>631</sup> 39 U.S.C. § 3661(b).

<sup>632</sup> *See id.* § 3361(b) (1988). On the "balance of powers" between the two bodies, *see U.S.P.S. Governors v. PRC*, 654 F.2d 108 (D.C. Cir. 1981). In *Governors*, the Postal Service submitted a mail classification proposal to add "E-COM" (Electronic Computer Originated Mail) services to the DMM Classification Schedule. In response, the PRC recommended that E-COM be designated as "experimental" with a fixed termination date. The court held that the PRC had no authority to make such a recommendation, which amounted to a variety of regulation, and instead recognized only a limited hearing and advisory role on the part of the PRC. *See also Buchanan v. U.S.P.S.*, 508 F.2d 259, 262-64 (5th Cir. 1975) (noting a policy of broad authority in postal management); *U.S.P.S., Inc. v. U.S.P.S.*, 455 F. Supp. 857 (E.D. Pa. 1978), *aff'd*, 604 F.2d 1370 (3rd Cir. 1979), *cert. denied*, 446 U.S. 957 (1980) (rejecting analogy between the P.R.C. and other regulatory agencies with broader mandates over private industry); *Air Courier Conference of Am. v. USPS*, 762 F. Supp. 86 (D. Del. 1991), *order aff'd*, 957 F.2d 1213 (3rd Cir. 1992) (USPS not required to submit desired rate changes for on-demand express mail int'l service to PRC for review and recommendation).

<sup>633</sup> *See Silver v. U.S.P.S.*, 951 F.2d 1033, 1036 (9th Cir. 1991) (substantiating that the U.S.P.S. "is not an organization independent of the U.S. government").

and subcommittees have influence over Postal Service operations, including the Post Office Committee and the Civil Service Committee in the House and the Government Affairs Committee in the Senate. Other committees, such as the House Government Operations Committee, hold hearings from time to time on issues affecting the Postal Service.

The Postal Service has willingly participated in programs experimenting with digital signature technology, such as E-COM. The Postal Service pursued the E-COM proposal with the support of the Administration, following a Presidential Review Memorandum and subsequent Administration Policy Statements issued on July 19, 1979 without arousing legislative opposition.<sup>634</sup> The service was eventually terminated, in part, because of an inability to establish a viable rate for the service.

Messaging in all its forms -- traditional and computer-based -- is a competitive business and private companies would have to be taken into account in any FCA plan. Communications giants like AT&T, who would probably control a significant portion of the electronic infrastructure needed, will likely demand a significant role. The competitive and political obstacles may be significant. On the other hand, a number of European postal authorities already engage in EDI and have plans to increase electronic mail and hybrid mail services. The political landscape is complex, but solutions can and will be found. The extent to which the Universal Postal Union (UPU) or other inter-postal authority endeavors would lead to the adoption of USPS international electronic commerce products.

### **Potential Liability**

A considerable quantity of rhetorical ink has been spilled on the commercialized nature, and concomitant exposure to liability, of the Postal Service as reconstituted by the PRA.<sup>635</sup> The Supreme Court has noted that Congress "wished

---

<sup>634</sup> See generally, Electronic Mail Classification Proposal, 1978, Docket No. MC 78-3 (PRC, Dec. 17, 1979) (Recommended Decision) (determining establishment of E-COM services a mere matter of classification and noting unproblematic nature of Postal Service's entry into this area). It should be noted, however, that E-COM was a bulk service provided directly to the public and was similar to the "traditional" Mailgram service. As with Mailgram, E-COM was designed to convey electronic messages for "hard copy" delivery by ordinary means. See *Governors*, 654 F.2d at 110.

<sup>635</sup> See 39 U.S.C. § 401. The "General Powers of the Postal Service" include those "to sue and be sued"; to contract in its own behalf; to manage its financial affairs; to acquire property; and to settle and compromise claims.



the Postal Service to be run more like a business than had its predecessor, the Post Office Department."<sup>636</sup> The power "to sue and be sued," in particular, has been construed upon numerous occasions as constituting a waiver of sovereign immunity.<sup>637</sup>

However, this "commercial business" rhetoric has not dislodged the well established principle that the Postal Service is immune from liability in the handling of postal matter. While Congress provided a general waiver of immunity for the Postal Service in the PRA, it specifically retained sovereign immunity as to postal matter. Section 409(c) provides:

The provisions of Chapter 171 and all other provisions of Title 28 relating to tort claims shall apply to tort claims arising out of activities of the Postal Service.

"Chapter 171" refers to the Federal Tort Claims Act.<sup>638</sup> Among the exceptions to the FTCA's waiver of sovereign immunity is the following:

The provisions of this chapter and section 1346(b) of this title shall not apply to:

---

<sup>636</sup> *Franchise Tax Bd. v. U.S.P.S.*, 467 U.S. 512, 519-20 (1983).

<sup>637</sup> *Loeffler v. Frank*, 486 U.S. 549, 554-557 (1988); *Franchise Tax Bd.*, 467 U.S. 512. Both *Loeffler* and *Franchise Tax Bd.* quoted extensively from and relied upon *F.H.A. v. Burr*, 309 U.S. 242 (1940):

. . . when Congress establishes . . . an agency, authorizes it to engage in commercial and business transactions with the public, and permits it to "sue and be sued," it cannot be lightly assumed that restrictions on that authority are to be implied. Rather if the general authority to "sue and be sued" is to be delimited by implied exceptions, it must be clearly shown that certain types of suits are not consistent with the statutory or constitutional scheme, that an implied restriction of the general authority is necessary to avoid grave interference with the performance of a governmental function, or that for other reasons it was plainly the purpose of Congress to use the "sue and be sued" clause in a narrow sense. In the absence of such showing, it must be presumed that when Congress *launched a governmental agency into the commercial world* and endowed it with authority to "sue and be sued," that agency is not less amenable to judicial process than a private enterprise under like circumstances would be.

*Id.* at 245 (emphasis added).

<sup>638</sup> See generally Section VII.A.3.a., *supra*.

(b) any claim arising out of the loss, miscarriage, or negligent transmission of letters or postal matter.

By providing that the FTCA would be applicable to the reorganized Postal Service, Congress clearly intended that the immunity enjoyed by its predecessors for loss of mail would continue to apply to the federal defendant. "Congress never repealed 28 U.S.C. § 2680(b). Congress may have launched the Postal Service into the commercial world, but it did not send it off to fly alone. Congress maintained the Postal Service under the protective wing of § 2680(b) of the FTCA."<sup>639</sup>

Courts have been reluctant to condone attempts to circumvent the FTCA's "postal matter" exception by recharacterizing the relationship as contractual.<sup>640</sup> Even when there is or may be a contractual relationship with the Postal Service, courts have refused to hold it liable "except as may be provided in the postal laws and regulations."<sup>641</sup>

Those courts which have faced the issue whether the Postal Service may be liable for lost mail since the reorganization of 1970 have uniformly held that regardless of how the federal defendant's function is characterized, *i.e.*, governmental or commercial, it is still immune from the type of suit involved here.

For example, in *Allied Coin Investment, Inc.*, the plaintiff sent rare coins by Express Mail from Michigan to Minnesota. The coins never arrived. Plaintiff framed his complaint in theories of negligence, and characterized the Postal Service as a common carrier, a commercial bailee, and a party to an express contract. In granting the Postal Service's motion for summary judgment, the district court concluded that "while the characterization of the USPS as a common carrier, or a commercial bailee, or a party to an express contract is artful - the ultimate claim of liability remains misdelivery."<sup>642</sup>

---

<sup>639</sup> *Allied Coin Inv., Inc. v. U.S.P.S.*, 673 F. Supp. 982, 985.

<sup>640</sup> *See id.* at 986-87 (D. Minn. 1987).

<sup>641</sup> *Marine Ins. Co., Ltd. v. United States*, 410 F.2d 864, 766 (Ct. Cl. 1969). A good example of a situation in which the Postal Service might have been held liable for breach of its indemnification contract concerning a piece of registered mail may be found in *Frank Mastolini & Sons v. U.S.P.S.*, 546 F. Supp. 415 (S.D.N.Y. 1982) (plaintiff's failure to schedule full value of mis-delivered parcel rendered indemnification contract void; tort claim barred by FTCA).

<sup>642</sup> *Allied Coin*, 673 F. Supp. at 986.



Other courts have universally upheld sovereign immunity with respect to lost mail claims. For example, in *Anderson v. United States Postal Service*,<sup>643</sup> the plaintiff sent several of his original musical compositions from one Miami address to another by registered mail. On the same day, robbers held up a postal carrier and stole the mail, including Anderson's package. Anderson brought suit asserting claims for tort and breach of an insurance contract. The district court dismissed Anderson's tort claim for lack of subject matter jurisdiction, granted the Postal Service's motion for partial summary judgment on the issue of contract damages, and entered judgment in favor of Anderson for \$100.00 (the applicable amount of insurance allowed by postal regulations). The district court's ruling was affirmed by the Ninth Circuit:

The Federal Tort Claims Act grants a waiver of sovereign immunity in certain cases. 28 U.S.C. § 1346(b). However, by 28 U.S.C. § 2680(b) the United States retains sovereign immunity for tort claims against it for "loss, miscarriage, or negligent transmission of the mails."<sup>644</sup>

Similarly, *Insurance Company of North America v. United States Postal Service*<sup>645</sup> involved a plaintiff who brought suit because a bag of currency did not reach its destination after being sent by registered mail. Suit was brought on both contract and tort theories. The district court dismissed the tort claims on a theory of sovereign immunity and granted summary judgment for the federal defendant on the contract claim. The plaintiff appealed the dismissal of the tort claim, but its appeal was rejected by the Fifth Circuit because "Section 2680(b) retains sovereign immunity with respect to claims of negligent handling of the mails."<sup>646</sup>

Since the passage of the Postal Reorganization Act of 1970, courts have limited the Postal Service's general protection under the doctrine of sovereign immunity, but this has been under those circumstances when a statute was not involved.<sup>647</sup> None of the cases which have limited the Postal Service's sovereign immunity

---

<sup>643</sup> 761 F.2d 527 (9th Cir. 1985).

<sup>644</sup> *Id.* at 528.

<sup>645</sup> 675 F.2d 756 (5th Cir. 1982).

<sup>646</sup> *Id.* at 759.

<sup>647</sup> See *Portmann v. United States*, 674 F.2d 1155 (7th Cir. 1982) (doctrine of equitable estoppel applicable against Postal Service under certain circumstances); *May Dep't. Stores Co. v. Williamson*, 549 F.2d 1147 (8th Cir. 1977) (Postal Service not immune from garnishment procedures to effect judgment in state courts.).

have involved the explicit provision provided by Congress under the FTCA.<sup>648</sup> It is clear that the Postal Service is liable to the owners of lost or damaged mail only to the extent to which it has consented to be liable, and the extent of its liabilities are defined by postal laws and regulations.<sup>649</sup>

Further, the government is not liable, even assuming that an implied contract of bailment exists between the government and a sender by virtue of a mailing, for loss of or damage to mail, except as may be provided in postal laws and regulations.<sup>650</sup>

### **The Possibilities for Post Office Liability**

As the preceding discussion indicates, most of the potential liability for an FCA administered by the Post Office will depend on whether FCA functions are deemed "postal matter." If so, the FCA would be immune from liability suits based on negligent performance of those services. However, if FCA functions do not constitute "postal matter," the waivers of sovereign immunity pursuant to both the PRA and the FTCA will likely create liability exposure.

To determine whether FCA services are "postal matter," it is useful to examine two other partially electronic experimental services: E-COM and Mailgram. The USPS considered both E-COM and Mailgram as subclasses of first class mail.<sup>651</sup> Although the FCA does not actually send paper through the mails (except perhaps as an ancillary support function, such as for certificate application forms and confirmatory purposes) as do E-COM and Mailgram, its *facilitation* of the transfer of electronic mail by establishing authenticity and reliability services make it somewhat analogous.

---

<sup>648</sup> The Eighth Circuit itself recognized this basic distinction. *See May Dep't*, 549 F.2d at 1149 n.2 (noting that Congress restricted consent to suit against Postal Service by applicability of FTCA).

<sup>649</sup> *See Twentier v. United States*, 109 F. Supp. 406, 408-09 (Cl. Ct. 1953); *accord Marine Ins. Co. v. United States*, 410 F.2d 764, 766 (Cl. Ct. 1969) (Government's motion for summary judgment granted); *Frank Mastolini & Sons v. U.S.P.S.*, 546 F. Supp. 415, 419 (S.D. N.Y. 1982) (Postal Service is only liable to the extent it agrees to be liable).

<sup>650</sup> *See Marine Ins. Co. v. United States*, 410 F.2d at 764 (1969).

<sup>651</sup> *See U.S.P.S. Governors v. P.R.C.*, 654 F.2d 108, 110 (D.C. Cir. 1981); *United Tel. Workers v. FCC*, 436 F.2d 920 (D.C. Cir. 1970).



It is arguable that an FCA's functions are of a primarily commercial nature. In some ways, these sorts of commercial functions might have been exactly what Congress had in mind when it made the Postal Service amenable to suit under the PRA. As this Report argues elsewhere, potential liability induces efficiency, integrity and trust, which are three attributes an effective FCA must possess and inspire. However, in order to keep such liability within reasonable limits, the FCA should develop and execute liability regimes, by regulation, agreement, or otherwise, which clearly define the limits on its liability. It should also consider offering insurance to users as the USPS does now.

Insurance limits could be based upon the needs of the primary users. The USPS currently offers varying insurance limits for its services. For express mail, the USPS offers insurance for non-negotiable documents of up to \$50,000 and of merchandise of up to \$500.<sup>652</sup> The insurance limit on registered mail is \$25,000.<sup>653</sup> Finally, customers can insure third and fourth class mail for up to \$600.<sup>654</sup> However, to the extent that public key certificates are viewed as primarily protecting the receiver rather than the sender of a digitally signed message, it may ultimately be necessary to put the burden of obtaining insurance on the receiver. In this respect, current USPS insurance schemes may not be of great practical use for FCA purposes.

#### **b. Federal Reserve System**

The Board of Governors of the Federal Reserve System or, more generally, the Federal Reserve System (collectively, the "Fed") has also been proposed as a repository for the FCA. Factors weighing in favor of such a disposition include its pervasive national presence; the existence of a similarly pervasive communications network; and, perhaps above all, its *trusted entity* status<sup>655</sup> and relative independence from political pressures.

---

<sup>652</sup> See USPS DOMESTIC MAIL MANUAL, *supra* note 615, § 295.21. Liability is further limited to \$500,000 per occurrence regardless of the number of mail items or the number of customers involved.

<sup>653</sup> See *id.* § 911.231.

<sup>654</sup> See *id.* §§ 913.12, 913.21.

<sup>655</sup> Mr. Herbert Whiteman, Director of Information Security for the N.Y. Federal Reserve Bank, has indicated that "if [performing FCA functions] falls on us, we'll do it." Telephone interview with Herbert Whiteman (May 1993). Mr. Whiteman added that the Fed "guard[s its trusted entity] status jealously," and noted that the General Accounting Office has unsuccessfully attempted to investigate the Fed in

## Authority to Undertake FCA Operations

The Fed probably lacks authority under currently applicable law to undertake generalized FCA services.<sup>656</sup> Further, although the Fed could likely implement all or part of any FCA infrastructure in its currently existing "Fedwire" funds transfer system,<sup>657</sup> any such implementation would presumably need to fall within the scope of the terms "deposits," "collections," "withdrawals," or "transfer of funds."<sup>658</sup> Accordingly, it is a virtual certainty that Congressional action would be a prerequisite to the Fed's performance of generalized FCA services.

## Relationship with the Private Sector

As will presumably be the case with any reasonably foreseeable FCA infrastructure, the Fed (alongside other regulatory institutions)<sup>659</sup> exercises both a regulatory role over, and a participatory role in, the system of privately operated banking institutions in the United States. This structure, in fact, likely constitutes *the* single most useful analog or pattern for the FCA infrastructure.

---

the past and that Fed security personnel require "top secret" government clearance. *Id.*

<sup>656</sup> See generally 12 U.S.C. §§ 248, 341.

<sup>657</sup> See 12 C.F.R. §§ 210.25 *et seq.* Fedwire is discussed in greater detail in Section VIII.A.5., *infra*.

<sup>658</sup> See 12 C.F.R. § 210.25(a) (citing 12 U.S.C. §§ 248(i), 248(o), 242, 464, from which the terms in the accompanying text are derived, as authority for promulgation of Fedwire regulations); *cf.* 12 C.F.R. §§ 225.25(b)(7) ("permissible nonbanking activities" include "[p]roviding to others data processing and data transmission services, facilities . . . data bases or access . . . if . . . the data to be processed . . . are financial, banking, or economic"); 225.123(e)(1) (permitting bank holding companies to provide "incidental" data processing services using excess capacity). Note that the Fed is not subject to the Bank Holding Company Act.

<sup>659</sup> These institutions include, most notably, the Comptroller of the Currency, *see* 12 U.S.C. §§ 21-220, and the Federal Deposit Insurance Corporation (the "F.D.I.C."), *see id.* §§ 1811-1834b. The F.D.I.C. is discussed briefly *infra*.



## Regulation

The Fed is comprised of the Board of Governors of the Federal Reserve System (the "Board") and twelve Federal Reserve Banks ("FRBs"), each of which is owned by the "member banks" within its territory. Membership in the Fed is required for national banks and is available to state-chartered<sup>660</sup> depository institutions. Members of the Board are selected for terms of fourteen years by the President of the United States, with the advice and consent of the Senate.<sup>661</sup> FRB boards of directors have nine members. Three are elected as representatives of member banks; three are elected as representatives of "the public"; and three are appointed by the Board.<sup>662</sup> Selection of FRB board members for the latter two categories is to be "with due but not exclusive consideration to the interests of agriculture, commerce, industry, services, labor and consumers."<sup>663</sup> "Said board[s] of directors shall administer the affairs of said [FRBs] fairly and impartially and without discrimination in favor of or against any member bank or banks . . . ."<sup>664</sup>

Financial risk to individual member banks and to the banking system generally is controlled by means both of positive law<sup>665</sup> and market-oriented incentives.<sup>666</sup> Although the Board has discretion to examine both FRBs and member banks,<sup>667</sup> examination of state-chartered member banks and of bank holding companies is ordinarily performed by the Board, while examination of nationally chartered banks is performed by the Comptroller of the Currency.<sup>668</sup>

---

<sup>660</sup> See *id.* §§ 321 *et seq.*

<sup>661</sup> See *id.* § 241.

<sup>662</sup> *Id.* § 302.

<sup>663</sup> *Id.*

<sup>664</sup> *Id.* § 301; see *Huntington Towers, Ltd. v. Franklin Nat'l Bank*, 559 F.2d 863 (2d Cir. 1977).

<sup>665</sup> See, e.g., 12 U.S.C. §§ 371c, 371c.1 (governing transactions with affiliates); *id.* §§ 375, 375a, 375b (transactions with executive officers and directors); *id.* 377 (securities activities); *id.* § 461 (reserve requirements).

<sup>666</sup> See Federal Reserve Policy Statement on Payments System Risk, 57 Fed. Reg. 40,455 (1992), as amended by Docket No. R.0668 (Oct. 6, 1992).

<sup>667</sup> See 12 U.S.C. § 248(a).

<sup>668</sup> See *id.* § 1844.

The Fed may levy a series of escalating civil penalties against member banks that violate certain prohibitions, "recklessly engage in an unsafe or unsound practice in conducting [its] affairs," or breach "any fiduciary duty."<sup>669</sup> The Fed may also direct proceedings for the dissolution of "any national banking association [that] fails[s] to comply with any of the provisions of the [Federal Reserve Act] applicable thereto."<sup>670</sup> Officers and directors of member banks face personal liability for damages to banks or to others for their actual or imputed violations of law.<sup>671</sup> Finally, certain duties on the part of institutions and individuals, including examiners, are enforced by criminal sanctions.<sup>672</sup>

---

<sup>669</sup> *Id.* §§ 504, 505. *See infra* note 1013 (concerning fiduciaries).

<sup>670</sup> *Id.* § 501a.

<sup>671</sup> *See id.* § 503; *see also id.* § 501a.

<sup>672</sup> *See, e.g.,* 18 U.S.C. §§ 212-215, 655, 1005, 1906, 1090.



## Participation

The Fed also performs myriad functions as a quasi-private participant in the nation's clearing and settlement systems. Thus, the Board may require FRBs "to exercise the functions of a clearing house for depository institutions."<sup>673</sup> In the course of exercising these functions, FRBs have become subject to various duties imposed by generalized payment systems law<sup>674</sup> and have bound themselves by instruments best described as "contractual" in nature to perform other duties in more particularized systems.<sup>675</sup> The Fed also competes with private entities in the provision of clearing and settlement services, and is required to charge fees for these services.<sup>676</sup>

It must be noted, however, that the Fed does not participate on an "even playing field." Under the Supremacy Clause of the United States Constitution,<sup>677</sup> the Fed may "opt out" of various provisions of state law.<sup>678</sup> The Fed's dual role is not without controversy,<sup>679</sup> but, on balance, doing away either with banking regulation or with the national unity and coherence afforded by the Fed's participation in the check clearing system, "Uniform" Commercial Code notwithstanding, is probably not practicable (or perhaps even desirable) in the short term. Splitting the functions among new or different agencies is another

---

<sup>673</sup> 12 U.S.C. § 248(o).

<sup>674</sup> See, e.g., *Northpark Nat'l Bank v. Bankers Trust Co.*, 572 F. Supp. 524, 528-529 (S.D.N.Y. 1983) (denying FRB's motion to dismiss claim for failing to exercise duty of ordinary care under Article 4 of the Uniform Commercial Code). Article 4 is discussed generally herein at Section VIII.A.1., *infra*.

<sup>675</sup> See, e.g., CHIPS Settlement Agreement, discussed *infra*, at Section VIII.A.4., and the Automated Clearing House Uniform Operating Circular, discussed *infra*, at Section VIII.A.3.

<sup>676</sup> See 12 U.S.C. § 248a.

<sup>677</sup> U.S. CONST. art. VI, cl. 2.

<sup>678</sup> See, e.g., 12 C.F.R. § 210.6(a)(a) ("A Reserve Bank shall not have or assume any liability . . . except for the Reserve Bank's own lack of good faith or failure to exercise ordinary care . . . "); *id.* § 210.25(a)("[T]his subpart is not a funds transfer system rule as defined in Section 4A-501(6) of Article 4A [of the Uniform Commercial Code]").

<sup>679</sup> See Association of Reserve City Bankers, *Report on the Payments System* 25-28 (1982).

alternative, but the United States' patchwork system of bank regulation probably requires nothing less than another bureaucracy.<sup>680</sup>

Because they are owned by (private) "member banks," FRBs are neither entitled to the benefits, nor subject to the burdens, of the FTCA.<sup>681</sup> Moreover, the broad regulatory schemes governing banking agencies and banks do not contain a basis for implying a duty of care running from the agencies to banks and their shareholders.<sup>682</sup>

### **The Federal Deposit Insurance Corporation (the "F.D.I.C.")**

Although the F.D.I.C. is, of course, not a part of the Fed, even a cursory examination of the banking system would be incomplete without a mention of it. In particular, the F.D.I.C. constitutes an important paradigm for governmentally-sponsored insurance for "end-users" (*i.e.*, depositors) of banking services, and for this reason is relevant to the FCA. Finally, the regime established for the F.D.I.C. contains certain pitfalls that should be avoided should an analogous institution or function be implemented with respect to the FCA.

The F.D.I.C. insures depositors against bank failure up to a maximum amount of \$100,000 per depositor, per account category, at each institution.<sup>683</sup> The deposits maintained in different categories of legal ownership are separately insured. The F.D.I.C. is financed primarily through periodic "assessments" and additionally by "entrance" and "exit" fees<sup>684</sup> on institutions becoming or ceasing to be "insured institutions."<sup>685</sup> The F.D.I.C. as well as Federal bank agencies are subject to comprehensive reporting requirements, both on the part of insured

---

<sup>680</sup> Title 12 of the United States Code currently governs approximately 10 separate regulatory institutions. In addition, every (or virtually every) state has at least one regulatory body having jurisdiction over banking services.

<sup>681</sup> See *Lewis v. United States*, 680 F.2d 1239 (9th Cir. 1982).

<sup>682</sup> See *In re Franklin Nat'l Bank Sec. Litig.*, 478 F. Supp. 210 (E.D.N.Y. 1979).

<sup>683</sup> See 12 U.S.C. § 1821(a)(1).

<sup>684</sup> *Id.* § 1815(d).

<sup>685</sup> *Id.* § 1817(b).



institutions,<sup>686</sup> and on the part of the F.D.I.C. (to Congress).<sup>687</sup> The system receives financial support from parties affiliated with insured institutions in a variety of ways. Thus, for example, insured institutions that are under common control with other insured institutions that have failed or are in danger of failing are liable for losses the F.D.I.C. incurs in connection with the liquidation or rehabilitation of the failed institution.<sup>688</sup> Further, the "appropriate Federal Banking agency"<sup>689</sup> has authority to issue "cease and desist" orders to insured institutions and "institution-affiliated party"<sup>690</sup> for actual and/or prospective "unsafe or unsound practices in conducting the business of such depository institution" or for violation of law.<sup>691</sup> The Federal Reserve Board is given separate authority to issue cease and desist orders to bank holding companies.<sup>692</sup> The F.D.I.C. may request other agencies to take protective action with respect to banks within their jurisdiction and, upon their failure to act, may take that action itself.<sup>693</sup>

Cease and desist orders may order "affirmative action," such as the making of restitution, reimbursement, or indemnification against loss if the recipient of the order was unjustly enriched or if the violation involved "reckless disregard" of applicable law.<sup>694</sup> In addition, insured institutions and institution-affiliated

---

<sup>686</sup> See *id.* §§ 1817(a), (c), 1831m.

<sup>687</sup> See *id.* § 1827.

<sup>688</sup> See *id.* § 1815(e)(1).

<sup>689</sup> *Id.* § 1813(q). Depending on the type of "bank involved," the "appropriate Federal banking agency" might be the Comptroller of the Currency; the Fed Board; the F.D.I.C. or the Director of the Office of Thrift Supervision. *Id.*

<sup>690</sup> *Id.* § 1813(a). The definition is slightly bizarre. It includes, *inter alia*, officers, directors, controlling shareholders -- but *not* -- bank holding companies, *cf. id.* 12 U.S.C. §§ 1841 *et seq.* ("The Bank Holding Company Act of 1956"), persons having filed "change-in-control" notices, and, in certain circumstances, "any independent contractor (including any attorney, appraiser or accountant)." *Id.* § 1813(a).

<sup>691</sup> *Id.* § 1818(b)(1).

<sup>692</sup> See *id.* § 1818(b)(3).

<sup>693</sup> See *id.* § 1818(t).

<sup>694</sup> *Id.* § 1818(b)(6). Interestingly, the statute states that the only insured institutions and institution-affiliated party, *see* note 690, *supra*, are subject to "affirmative action" orders. 12 U.S.C. § 1818(b)(6). The Federal Reserve Board,

parties are subject to a tiered sequence of penalties for violating cease and desist orders.<sup>695</sup>

Congress has recently harkened to two major complaints respecting the insurance scheme administered by the F.D.I.C. Any formal or *de facto* "insurance" services to be provided by the FCA should assiduously avoid falling into similar traps.

First, Congress has legislatively overruled the uncodified "too big to fail" doctrine,<sup>696</sup> which was widely perceived as unfair. Second, Congress has mandated that the F.D.I.C. institute, for the first time, risk-based assessments on banks for insurance.<sup>697</sup> Whether in the face of popular pressure these schemes will survive for long, or even become effective, remains to be seen.

### c. General Services Administration

As a practical matter, the General Services Administration (the "GSA") will likely be required to play an important role with regard to establishment of the FCA infrastructure. Under current law, the GSA Administrator is "authorized and directed to coordinate and provide for the economic and efficient purchase, lease, and maintenance of automatic data processing equipment by Federal agencies."<sup>698</sup>

---

linking together its authority under the Bank Holding Company Act and section 1818(b)(3), has sought to assert its authority to order bank holding companies to contribute funds to their failing subsidiaries. Cf. 12 C.F.R. § 225.4(1)(a) ("A bank holding company shall serve as a source of financial and managerial strength to its subsidiary banks."). This is the infamous "source of strength" doctrine the Supreme Court recently refused to review in *Board of Governors of the Fed. Reserve Sys. v. M Corp Fin., Inc.*, 112 S. Ct. 459 (1991).

<sup>695</sup> See 12 U.S.C. § 1818(i).

<sup>696</sup> See *id.* § 1823(c)(4)(e) (effective Dec. 31, 1994). Nonetheless, discretion remains for application of the doctrine to avoid "serious adverse effects on economic conditions or financial stability." *Id.* § 1823(c)(4)(G).

<sup>697</sup> Pub. L. No. 102-242, § 302(a), (g), 105 Stat. 2345, 2349 (1991), as amended, Pub. L. No. 102-558, § 303(a), (b)(7)-(8) (1992) (amending 12 U.S.C. § 1817(b)) (effective Jan. 1, 1994).

<sup>698</sup> 40 U.S.C. § 759(a)(1). "Automatic data processing equipment" is defined broadly to include hardware, software, services and "other resources" "used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information" by or under contract with federal agencies. See *Id.* § 759(a)(2).



More generally, the GSA may perform useful functions in the FCA to the extent that it has a history of providing procurement and other services to the federal government, including the procurement of the "FTS-2000" telecommunications services<sup>699</sup> provided by Sprint Telecommunications, Inc. and AT&T, and the Secure Packet Switch Service Offering.<sup>700</sup>

The GSA currently evaluates the credentials of several hundred thousand government vendors for procurement certification purposes. The GSA also maintains a "disbarred certificate list," which might be viewed as a conventional analog to a CRL. It is also the provider of emergency telecommunications services to the Federal Emergency Management Agency ("FEMA") and, as such, has experience in ensuring reliability and availability.

In keeping with informal initiatives within the GSA to be more "service-oriented" and its current provision of cryptographic key management services to the government (and therefore its demonstrated role as an experienced *trusted entity*), it should be kept in mind as a potential provider of FCA services, and, in any event, should be an important contributor to FCA policy development.

On the other hand, the GSA's authority at present does not appear to go far beyond procurement contracting.<sup>701</sup> In addition, it has little history of providing services to the public generally<sup>702</sup> and does not exhibit the pervasive presence and availability of, for example, the Postal Service and the Fed. Nonetheless, the GSA demonstrates a potential to provide highly secure services.

---

Excluded from the scope of the section, however are, *inter alia*, certain procurements by the Department of Defense and the Central Intelligence Agency. *Id.* § 759(a)(3). The GSA has promulgated the so-called "Federal Information Management Regulations System" (the "FIRMR"), *See* 41 C.F.R. §§ 201-1.000 *et seq.*, in pursuance of the authority and duty devolved upon it by section 759(a).

<sup>699</sup> In this respect the FCA may benefit from the GSA's knowledge of and experience with VANs; regulatory rules and policy; and the availability and constraints associated with enhanced telecommunications services.

<sup>700</sup> This provides unclassified but sensitive key management. *See* FIRMR Bulletin 37, Rev. 1 ("Communications security (COMSEC) and related telecommunications equipment service rates") (describing various GSA COMSEC services).

<sup>701</sup> *See generally* 40 U.S.C. § 752.

<sup>702</sup> One exception is its role as manager of the Federal Information Centers. *See id.* § 760.

#### d. National Institute of Standards and Technology

The National Institute of Standards and Technology ("NIST"), like the GSA, will also be required to play a role in the FCA infrastructure. Pursuant to the Computer Security Act of 1987,<sup>703</sup> NIST has been directed to develop *standards and guidelines* to be incorporated into the Federal Information Resource Management Regulation ("FIRMR").<sup>704</sup>

More generally, not least because of its development of the Digital Signature Standard ("DSS"),<sup>705</sup> NIST is, and will for the foreseeable future be, a *de facto* focal point for any federal effort in the certification area. NIST's pre-eminent role in the nation's technical standards, its mandate for interaction with the private sector<sup>706</sup> and its placement within the Department of Commerce<sup>707</sup> give it a unique vantage point from which to coordinate FCA initiatives with commercial, law enforcement and national security interests of the federal government and the interests of the private sector.<sup>708</sup>

NIST's operation of the National Voluntary Laboratory Accreditation Program gives it experience in functions closely analogous to those of PCAs. Although NIST is not currently authorized or equipped to handle FCA functions in the quasi-private, "commercial" manner demanded by effective liability schemes, and may not, out of a sense of scientific integrity, wish to do so, it must certainly be a candidate at least for a high-level function within the FCA and should perhaps play a technical role in its operation as well. Moreover, its cooperative research consortium initiatives<sup>709</sup> "for secure software encryption with integrated

---

<sup>703</sup> Pub. L. No. 100-235, 101 Stat. 1727 (1988).

<sup>704</sup> 41 C.F.R. §§ 201-1.000 *et seq.* (promulgated pursuant to 40 U.S.C. § 759(d)).

<sup>705</sup> See 56 Fed. Reg. 42,981 (Aug. 30, 1991).

<sup>706</sup> *Id.*

<sup>707</sup> *Id.*

<sup>708</sup> See especially 15 U.S.C. § 278g-4 (establishing the public, commercial and private "Computer System Security and Privacy Advisory Board" (CSSPAB) to advise NIST on "security and privacy issues pertaining to Federal computer systems").

<sup>709</sup> The initiatives have been undertaken pursuant to the Federal Technology Transfer Act of 1986, 15 U.S.C. § 3710a.



cryptographic key escrowing techniques," demonstrates the multi-dimensional activities relevant to the FCA.<sup>710</sup> Finally, the central role that NIST has shouldered in pioneering the coordination and study of the FCA infrastructure demonstrates a level of expertise and commitment unparalleled by any other government entity.

#### **e. Other Domestic Entities**

There are other federal agencies that deserve consideration as worthy contributors/participants to the FCA infrastructure. These agencies include the Financial Management Services<sup>710A</sup> and the U.S. Customs Service.

The U.S. Customs Service has emphasized automation as a primary means for implementing the Customs Modernization Act of 1993.<sup>710B</sup> It also serves as the enforcement mechanism for a considerable array of other regulations affecting the import and export of goods. Customs requirements are critical for harmonizing commercial documentation, such as those under the North American Free Trade Agreement ("NAFTA"). For example, Customs has undertaken a fairly comprehensive overhaul of its procedural requirements from private commercial documents (*i.e.* bills of lading, invoices, etc.) to public law (mandating required documents such as Certificates of Origin) (*see* Section VIII.E.3., *infra.*) that will have an impact on international trade. Furthermore, Customs has worked closely with other customs authorities internationally under the auspices of the Customs Coordination Council ("CCC"), and other organizations.<sup>710C</sup>

The functions of Customs exhibit certain attributes of a CA (*e.g.*, its inspection validates or authenticates the veracity of commercial documents). This role will likely become more important as Customs' anticipated EDI capabilities increase. Furthermore, Customs' administrative review procedures and decisions

---

<sup>710</sup> 58 Fed. Reg. 44,662 (Aug. 24, 1993).

<sup>710A</sup> *See generally* Section VIII.A., *infra* (concerning financial regulation generally).

<sup>710B</sup> Pub. L. No. 103-182.

<sup>710C</sup> *See* ELECTRONIC CONTRACTING, *supra* note 2, § 11.11, at 697-99 (discussing Customs use of EDI); 58 Fed. Reg. 12,878 (to be codified at 19 C.F.R. pt. 4) (Mar. 18, 1994) (proposing the extended use of EDI to facilitate "preliminary entry" of U.S. or foreign vessels) ]. Regulatory authority for EDI-based Customs activity is found in 19 C.F.R. pts. 111, *et seq.*

concerning valuation and classification issues provide guidance on certain liability issues of potential relevance to the FCA.

## 5. International Organizations Generally

This subsection considers possible roles of international organizations<sup>711</sup> in respect of FCA-like services, including service as a registration authority<sup>712</sup> or a

---

<sup>711</sup> An international organization is defined as "an organization that is created by an international agreement and has a membership consisting entirely or principally of states." RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 221 (1987) [hereinafter RESTATEMENT 3D]; *cf. id.* § 221, cmt. a ("Transnational entities established by national law or by agreement between private parties are not international organizations as here defined.") "Whether an activity undertaken jointly by states is an organization with international personality may be a matter of degree." *Id.* § 221 cmt. b. "An international organization such as the European Economic Community [Union] may in turn be a member of another international organization." *Id.* § 221 cmt. c. An entity such as the General Agreement on Tariffs and Trade (GATT) is a "continuing agreement" rather than an international organization although "a limited legal personality has evolved." *Id.* § 221 Rep. Notes 2. Compare this with INTELSAT (a public international corporation created by agreement); *see id.* § 221 Rep. Notes 3; *see also* Weidner v. International Telecommunications Satellite Org., 392 A.2d 508 (D.C. App. 1978).

Under the International Organizations Immunities Act of 1945 (the "IOIA") an "international organization" means:

. . . a public international organization in which the United States participates pursuant to any treaty or under the authority of any Act of Congress authorizing such participation or making an appropriation for such participation, and which shall have been designated by the President through appropriate Executive order as being entitled to enjoy the privileges, exemptions, and immunities provided in this subchapter. The President shall be authorized, in the light of the functions performed by any such international organization, by appropriate Executive order to withhold or withdraw from any such organization or its officers or employees any of the privileges, exemptions, and immunities provided for in this subchapter (including the amendments made by this subchapter) or to condition or limit the enjoyment by any such organization or its officers or employees of any such privilege, exemption, or immunity. The President shall be authorized, if in his judgment such action should be justified by reason of the abuse by an international organization or its officers and employees of the privileges, exemptions, and immunities provided in



vehicle to convey a certain "international status" on non-governmental organizations or as providers of accreditation or certification services.<sup>713</sup> For these purposes, this subsection considers the privileges and immunities of international organizations generally, such as the United Nations ("UN"), for their impact on FCA-relevant registration activities and certain other international organizations that have contributed to "registration authority" development: the International Standards Organization ("ISO") and the

---

this subchapter or for any other reason, at any time to revoke the designation . . . .

22 U.S.C. § 288. The list of international organizations so designated appears at 22 U.S.C.A. § 288, Historical note.

<sup>712</sup> See, e.g., note 12, *supra* (containing a figure of one proposed hierarchy susceptible to such forms of registration -- where "registration" is undertaken by the TLCA).

Registration [for an assignment] could take place in an international register or in a central national register accessible through an international centralized data base. An international register would facilitate both registration and access to registered information. Moreover, the legal framework for such an international register would require a set of uniform rules that in all likelihood would need to be in the form of a convention. As to the concerns related to cost of establishment and operation of an international register, simplicity and ease of registration and access to information registered in an international register, a way to alleviate those concerns, at least in part, might be to establish an international registration system with a United Nations agency as a registration authority, which would make use of existing means and would be accessible throughout the world due to the universal nature of the United Nations. In case the establishment of an international register proves to be not feasible, a central international data bank might be established so that the information filed at national registers could be made available to international users through modern means of communication.

UNCITRAL, Report of the Secretary General on the work of the 27th sess. concerning Possible Future Work on Legal Aspects of Receivables Financing (A/CN.9/397) (Apr. 29, 1994), ¶ 46, at 15.

<sup>713</sup> See Section IX.A.7. ("Potential FCA Certification and Accreditation Bodies"), *infra*.

International Telecommunications Union (the "ITU").<sup>714</sup> Certain other international organizations of a sectoral scope that may contribute in a limited way in the developing secure infrastructure are identified.

At the outset, however, it is important to bear in mind that attempts at centralized, global registration have tended to fail. Consequently, recognition of a *family or community* of registration authorities under primarily national (rather than international) control is more firmly grounded in historical and practical reality and demonstrated success. Also, fundamental questions require resolution, such as whether an international organization or a treaty is even necessary (as opposed to informal cooperation among national authorities). In this regard, one must consider the *level* at which responsibility needs to be taken.

#### **a. Privileges and Immunities**

"[A]n international organization generally enjoys such privileges and immunities from the jurisdiction of a member state as are necessary for the fulfillment of the purposes of the organization, including immunity from legal process, and from financial controls, taxes, and duties."<sup>715</sup> Some experts have asserted that "[b]roadly speaking, international organizations are immune from every form of legal process except insofar as that immunity is expressly waived by treaty or expressly limited by statute."<sup>716</sup>

General principles of liability of international organizations under United States law are codified, in part, from the Foreign Sovereign Immunities Act of 1976 ("FSIA")<sup>717</sup> and the International Organizations Immunities Act of 1945 (the

---

<sup>714</sup> Telecommunications law has been recognized as "one of the oldest branches of modern functional international law." E. PLOMAN, *INTERNATIONAL LAW GOVERNING COMMUNICATIONS AND INFORMATION* 227 (1982).

<sup>715</sup> RESTATEMENT 3D, *supra* note 711, § 467.

<sup>716</sup> 48 C.J.S. *International Law* § 67 (1981) (citing *Broadbent v. Organization of Am. States*, 481 F. Supp. 907 (D.D.C. 1978), *aff'd*, 628 F.2d 27 (D.C. Cir. 1980)).

<sup>717</sup> Pub. L. No. 94-583, 90 Stat. 2892 (1976) (codified in various provisions of Title 28, United States Code); *cf.* CONVENTION ON THE PRIVILEGES AND IMMUNITIES OF THE UNITED NATIONS, 13 FEBRUARY 1946, 21 U.S.T. 1418 (1970). Relevant portions of this convention include:

Art. II, § 2: "The United Nations, its property and assets wherever located and by whomever held, shall enjoy immunity from every form of legal process except insofar as in any particular case it has expressly waived its immunity."



"IOIA").<sup>718</sup> The U.S. Constitution provides a role for international bodies through the treaty making powers delineated in Article II, Section 2, Clause 2.<sup>719</sup> International organizations are "persons" in international law<sup>720</sup> and enjoy specified privileges and immunities by international agreement and accordingly only in relation to parties to those agreements, or under state legislation such as that of the United States.<sup>721</sup> Nonetheless, immunity should not be considered a license for lawless conduct:

In principle, an organization can also claim immunity from the application of other laws, if such immunity is necessary for the fulfillment of the organization's purposes . . . . [However] the organization is obligated generally to obey the law of the state in which it has its headquarters or conducts other activities, even if it is immune from legal process to enforce that law.<sup>722</sup>

---

Art. II, § 3: "The premises of the United Nations shall be inviolable."

Art. II, § 4: "The archives of the United Nations, and in general all documents belonging to it or held by it, shall be inviolable wherever located."

Art. III, § 10: "The United Nations shall have the right to use codes and to despatch and receive its correspondence by courier or in bags, which shall have the same immunities and privileges as diplomatic couriers and bags."

Art. V, § 18(a): "Officials of the United Nations shall: (a) be immune from legal process in respect of words spoken or written and all acts performed by them in their official capacity."

Art. VII, § 28: " The provisions of this article may be applied to the comparable officials of specialized agencies if the agreements for relationships made under Article 63 of the Charter so provide."

<sup>718</sup> 22 U.S.C. §§ 288 *et seq.*

<sup>719</sup> This clause provides that: "[The President of the United States] shall have power, by and with the advice and consent of the Senate, to make treaties . . . ." U.S. CONST. art. II, § 2, cl. 2; *cf.* 39 U.S.C. § 407a (authorizing the United States Postal Service, "with consent of the President, to negotiate and conclude postal treaties and conventions"); *CUNO Inc. v. Pall Corp.*, 729 F. Supp. 234, 240 (E.D.N.Y. 1989).

<sup>720</sup> See RESTATEMENT 3D, *supra* note 711, § 201.

<sup>721</sup> See *id.* § 467 cmt. a.

<sup>722</sup> See *id.* § 467 cmt. c.

## Commercial vs. Non-Commercial Activities

The FSIA states that "[u]nder international law, states are *not* immune from the jurisdiction of foreign courts insofar as their commercial activities are concerned, and their commercial property may be levied upon for the satisfaction of judgments rendered against them in connection with their commercial activities."<sup>723</sup> "Commercial activity" is defined as:

either a regular course of commercial conduct or a particular commercial transaction or act. The commercial character of an activity shall be determined by reference to the nature of the conduct or particular transaction or act, rather than by reference to its purpose.<sup>724</sup>

The FSIA then provides that:

(a) A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case . . .

(2) in which the action is based upon a commercial activity . . .<sup>725</sup>

[and] shall be liable in the same manner and to the same extent as a private individual under like circumstances; but a foreign state except for an agency or instrumentality thereof shall not be liable for punitive damages . . .<sup>726</sup>

The IOIA "authorizes the President, by executive order, to withdraw or reduce the immunities of international organizations under the IOIA. The possibility of limiting the immunity of an organization engaged in commercial activities was expressly contemplated, notwithstanding the potential applicability of the 'restrictive theory' of sovereign immunity."<sup>727</sup>

---

<sup>723</sup> 28 U.S.C. § 1602 (emphasis added).

<sup>724</sup> *Id.* § 1603(d).

<sup>725</sup> *Id.* § 1605(a)(2).

<sup>726</sup> *Id.* § 1606.

<sup>727</sup> RESTATEMENT 3D, § 467 Rep. Notes 1. The "restrictive theory" of immunity distinguishes "between the government or sovereign activities of a state (acts *jure imperii*) [for which there is immunity] and commercial activities (acts *jure gestionis*) [for which there is no immunity]." *Broadbent v. Organization of Am. States*, 628 F.2d 27, 30 (D.C. Cir. 1980).



## The United Nations

The United Nations<sup>728</sup> and its specialized agencies,<sup>729</sup> and regional and other major organizations, are generally considered to have international legal personality vis-à-vis all states (including non-member states), and these organizations are commonly deemed to enjoy privileges and immunities in relation to non-member states as a matter of customary law.<sup>730</sup>

The U.N. Charter provides that "[t]he Organization shall enjoy in the territory of each of its Members such legal capacity as may be necessary for the exercise of its functions and the fulfillment of its purposes."<sup>731</sup> The United Nations charter provides "immunity from every form of legal process" for the United Nations. It further provides that "The Organization shall enjoy in the territory of each of its

---

<sup>728</sup> The U.N. Charter was signed on June 26, 1945. The purposes of the U.N. are:

1. To maintain international peace and security . . .
2. To develop friendly relations among nations . . .
3. To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character . . . and
4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

U.N. CHARTER, Ch. I., art. 1.

<sup>729</sup> See U.N. CHARTER, arts. 57, 63. Article 63 provides:

1. The Economic and Social Council may enter into agreements with any of the agencies referred to in Article 57, defining the terms on which the agency concerned shall be brought into relationship with the United Nations. Such agreements shall be subject to approval by the General Assembly.
2. It may co-ordinate the activities of the specialized agencies through consultation with and recommendation to such agencies and through recommendations to the General Assembly and to the Members of the United Nations.

<sup>730</sup> See RESTATEMENT 3D, *supra* note 711, § 407 cmt. 1 (citing § 223 cmt. e).

<sup>731</sup> U.N. CHARTER, art. 104.

Members such privileges and immunities as are necessary for the fulfillment of its purposes."<sup>732</sup>

Concerning the immunity of the U.N.'s specialized agencies,

[s]ince the Convention on Privileges and Immunities of the United Nations exempts the United Nations 'from every form of legal processes,' conflict with United States Obligations under the Convention can be avoided only by interpreting the Foreign Sovereign Immunities Act as not applying to suits against the United Nations . . . Although the United States is not party to the parallel convention for the Specialized Agencies or that for the Organization of American States, those organizations were accorded privileges and immunities in their charters by language similar to that applicable to the United Nations in the United Nations Charter, and it is clear that these organizations were intended to have similar privileges and immunities. It is plausible, therefore, that the Foreign Sovereign Immunities Act, and the restrictive theory, should not be applied to those organizations either.<sup>733</sup>

International organizations "enjoy the same immunity from suit and every form of judicial process as is enjoyed by foreign governments, except to the extent that such organizations may expressly waive their immunity for the purpose of any proceedings or by the terms of any contract."<sup>734</sup>

International organizations shall enjoy the status, immunities, exemptions, and privileges set forth in this section, as follows:

(a) International organizations shall, to the extent consistent with the instrument creating them, possess the capacity-

(i) to contract;

(ii) to acquire and dispose of real and personal property;

(iii) to institute legal proceedings.

(b) International organizations, their property and their assets, wherever located, and by whomever held, shall enjoy the same immunity from suit and every form of judicial process as is enjoyed by foreign governments, except to the extent that such organizations may expressly waive their immunity for the purpose of any proceedings or by the terms of any contract.

(c) Property and assets of international organizations, wherever located and by whomever held, shall be immune from search, unless such immunity be expressly

---

<sup>732</sup> U.N. CHARTER art. 105(1); *see* U.N. Headquarters Agreement, 22 U.S.C.A. § 287 note.

<sup>733</sup> RESTATEMENT 3D, *supra* note 711, § 467 (citing *Broadbent v. Organization of Am. States*, 628 F.2d 27, 30 (D.C. Cir. 1980)).

<sup>734</sup> IOIA, 22 U.S.C. §§ 288-288f. Consideration of the "restrictive theory" of liability, which limits immunity to non-commercial activities is thought not to apply where, *e.g.*, the immunity of the United Nations expressly extends to "every form of legal process."



waived, and from confiscation. The archives of international organizations shall be inviolable.

(d) Insofar as concerns customs duties and internal-revenue taxes imposed upon or by reason of importation, and the procedures in connection therewith; the registration of foreign agents; and the treatment of official communications, the privileges, exemptions, and immunities to which international organizations shall be entitled shall be those accorded under similar circumstances to foreign governments.<sup>735</sup>

Absent objection from the Secretary General, the local law of the jurisdiction within which a U.N. entity is located applies.<sup>736</sup>

### **Immunity of Employees; Status of Independent Contractors**

The IOIA provides that:

(a) Persons designated by foreign governments to serve as their representatives in or to international organizations and the officers and employees of such organizations . . . other than nationals of the United States, shall, insofar as concerns laws regulating entry into and departure from the United States, alien registration and fingerprinting, and the registration of foreign agents, be entitled to the same privileges, exemptions, and immunities as are accorded under similar circumstances to officers and employees, respectively, of foreign governments, and members of their families.

(b) Representatives of foreign governments in or to international organizations and officers and employees of such organizations shall be immune from suit and legal process relating to acts performed by them in their official capacity and falling within their functions as such representatives, officers, or employees except insofar as such immunity may be waived by the foreign government or international organization concerned.<sup>737</sup>

However, "[t]he immunity of an international organization does not generally extend to independent contractors engaged by the organization."<sup>738</sup> Pursuant to the International Organizations Immunity Act, an international organization

---

<sup>735</sup> 28 U.S.C. § 228a.

<sup>736</sup> See *People v. Weiner*, 378 N.Y.S.2d 966 (1976); 48 C.J.S. *International Law* § 64, at 106 (1981).

<sup>737</sup> 22 U.S.C. § 288d.

<sup>738</sup> RESTATEMENT 3D, *supra* note 711, § 467 Rep. Note 2 (citing S. Rep. No. 861, 79th Cong., 1st Sess. 2 (1945)); cf. *Herbert Harvey, Inc. v. N.L.R.B.*, 424 F.2d 770 (D.C. Cir. 1969) (independent contractor providing maintenance and operating services for World Bank is not so related to the functions of the Bank as to warrant exemption from National Labor Relations Act and jurisdiction of NLRB); see also Section VII.B.1. ("Federal Contractor Liability"); See C.J.S. *Treaties* § 16.21.

commences legal action under the terms of the legal instrument creating it.<sup>739</sup> The United Nations may, for example, sue in the U.S. courts.<sup>740</sup>

### **Intergovernmental Telecommunications Treaty Liability**

Treaties establishing intergovernmental organizations that affect telecommunications generally include exculpatory clauses that diminish the liability of such organizations. For example, the ITU constitution provides: "Members [as distinguished from organizations] accept no responsibility toward users of the international telecommunication services, particularly as regards claims for damages."<sup>741</sup> Similarly, the "Operating Agreement Relating to the International Telecommunications Satellite Organization" provides that:

Neither INTELSAT nor any Signatory, in its capacity as such, nor any director, officer or employee of any of them nor any representative to any organ of INTELSAT acting in the performance of their functions and within the scope of their authority, shall be liable to, nor shall any claim be made against any of them by, any Signatory of INTELSAT for loss or damages sustained by reason of any unavailability, delay or faultiness of telecommunications services provided or to be provided pursuant to the Agreement or this Operating Agreement.<sup>742</sup>

As to warranty disclaimers, *e.g.*, the Convention Establishing a European Organization for the Exploitation of Meteorological Satellites provides that: "EUMETSAT offers no warranty in respect to the services and products provided or to be provided pursuant to this Convention."<sup>743</sup>

---

<sup>739</sup> See 48 C.J.S. *International Law* § 67.

<sup>740</sup> See *Balfour, Guthrie & Co. Ltd. v. United States*, 90 F. Supp. 831 (N.D. Cal. 1950).

<sup>741</sup> ITU, Final Acts of the Additional Plenipotentiary Conference, Geneva, 1992, art. 25.

<sup>742</sup> Agreements Establishing the International Telecommunications Satellite Organization, Washington, D.C., Aug. 20, 1974, art. 18

<sup>743</sup> Geneva, May 24, 1983.



## B. THE FEDERAL GOVERNMENT AS CONTRACTOR FOR FCA SERVICES

### 1. Federal Contractor Liability

In *Boyle v. United Technology Corp.*,<sup>744</sup> the United States Supreme Court recognized a "federal contractor" defense to products liability suits against manufacturers supplying military equipment to the federal government. This defense has been extended by the lower courts to contractors supplying non-military equipment as well.<sup>745</sup> Although it is tempting to conclude that a generally applicable immunity for government contractors exists, no such immunity should be relied upon absent further judicial (or legislative)<sup>746</sup> activity.

The *Boyle* decision was framed in terms of preemption of the state law of products liability by virtue of the "federal interest" in seeing that governmental functions are performed. The *Boyle* opinion establishes three factors for application of the "contractor defense": (1) approval by the government of "reasonably precise specifications"; (2) conformance with those specifications; and (3) warning to the United States of latent risks inherent in use of the equipment.<sup>747</sup> The Court ultimately founded its decision on the "discretionary function" exception to the FTCA,<sup>748</sup> pursuant to which the government is, or should be, permitted to exercise its discretion to mandate specifications for equipment procurals without fear of bearing the costs of tort suits either directly or in terms of higher contract prices.<sup>749</sup>

Although the rationale in *Boyle* could theoretically be applied to all forms of government contracting, the case should not be relied upon by FCA contractors, for several reasons. First, the Court stated explicitly that it was not recognizing a generalized defense for all government contractors.<sup>750</sup> Second, there is good

---

<sup>744</sup> 487 U.S. 500 (1988).

<sup>745</sup> See, e.g., *Carley v. Wheeled Coach*, 991 F.2d. 1117 (3d Cir. 1993) (supplier of trucks to United States Postal Service).

<sup>746</sup> A number of legislative initiatives have been proposed and defeated recently. See *Boyle*, 487 U.S. at 515 n.1 (Brennan, J. dissenting).

<sup>747</sup> *Boyle*, 487 U.S. at 512.

<sup>748</sup> 28 U.S.C. § 2680(a). This provision is discussed at Section VII.A.3.a. ("Federal Tort Claims Act"), *supra*.

<sup>749</sup> See *Boyle*, 487 U.S. at 511-12.

<sup>750</sup> See *id.* at 505 n.1.

cause for viewing FCA contracts as sufficiently distinguishable from the contract in *Boyle*. The *Boyle* contract dealt with the procurement of a specific piece of equipment, and it is arguably unlikely that an FCA contract would contain "reasonably precise specifications" such as those commonly encountered in equipment procurement contracts.

Also, the opportunity for losses to arise from operational human error or malfeasance is greater in the FCA context. The *Boyle* case only addressed design defects. Although technical flaws may certainly be part of the FCA infrastructure, the government cannot exercise the type of direct contract over contractor personnel that it can over equipment specifications. Accordingly, the potential scope for application of the "discretionary function" analogy is considerably less for FCA contractors.

Given that the "contractor defense" should not be relied upon by FCA contractors, the issue arises whether the government would be liable for indemnification absent contractual provision to the contrary. Fortunately, this is a problem that can (and certainly should) be dealt with by contract. There can be no excuse for leaving the matter to judicial caprice.<sup>751</sup>

The FTCA does not waive sovereign immunity for claims arising in a foreign country. Because it is likely that the FCA will facilitate international information transfers, the applicability of the FTCA to those transfers will depend on some definition of where those electronic events "occurred." For purposes of the FTCA, any non-U.S. land mass, including, for example, ungoverned Antarctica, is a foreign country, regardless of whether the land was under the sovereignty of a particular country.<sup>752</sup>

---

<sup>751</sup> In this regard, it is interesting to note that the sole reference to indemnification provisions in the Federal Acquisition Regulations, pertains to "unusually hazardous or nuclear risks" in contracts entered into pursuant to special national defense powers conferred on the President during times of national emergency. See 48 C.F.R. § 50.403 (promulgated pursuant to 50 U.S.C. §§ 1431-1435). Other indemnification provisions are a matter of legislation. See, e.g., 42 U.S.C. § 2210 (indemnification for nuclear power plant operations), discussed at Section IX.B.3. ("Government Insurance Programs"), *infra*.

<sup>752</sup> See *Smith v. United States*, 113 S. Ct. 1178 (1993). *Smith* editorialized as to why the court chose to hear this case assuming that "FTCA claims arising in Antarctica (or outer space) [are] presumably modest. . . . Perhaps the answer [is] that the justices have adopted the 'Star Trek' creed, resolving 'to Boldly go where no man has gone before.'" *Out in the Cold*, A.B.A. J. (June 1993), at 44. Perhaps this issue also calls into question the *situs* of cyberspace.



## 2. Federal Contracting/Federal Acquisition Regulation (FAR)

### Authority; Scope and Structure of the FAR

The Federal Acquisition Regulation (the "FAR")<sup>753</sup> has been promulgated pursuant to the "Office of Federal Procurement Policy Act" of 1974, as amended (the "Procurement Policy Act").<sup>754</sup> Pursuant to section 404 thereof, the Procurement Policy Act has established the Office of Federal Procurement Policy (the "Office") "in" the Office of Management and Budget (the "OMB"). The Office's "Administrator" is appointed by the President and confirmed by the Senate. In 1988, the Procurement Policy Act was amended to provide for the promulgation of "a single government-wide procurement regulation" to be known as the FAR.<sup>755</sup> The Procurement Policy Act gives broad authority to the Administrator to "deny the promulgation of or rescind" procurement regulations of "any executive agency" if they are determined by the Administrator to be "inconsistent with the policies set forth in section 401."<sup>756</sup>

In furtherance of the foregoing, the Procurement Policy Act takes precedence over existing authorizations to issue procurement regulations at the agency level.<sup>757</sup> The Administrator is also authorized to "develop innovative procurement methods and procedures."<sup>758</sup> In the event the Administrator determines "that it is necessary to waive the application of any provision of law" to test "innovative procurement methods and procedures," section 413(b) directs that he request various House and Senate committees to "take such action as may be necessary to provide that such provision of law does not apply with respect to the proposed program."<sup>759</sup> The applicability of the prohibition on use of "legislative vetoes" in *I.N.S. v. Chadha*<sup>760</sup> to this provision is uncertain. It should also be noted at this

---

<sup>753</sup> 41 U.S.C. §§ 1.000 *et seq.* (1992).

<sup>754</sup> 41 U.S.C. §§ 401-424 (1988 & Supp. III 1991).

<sup>755</sup> *Id.* § 405.

<sup>756</sup> *Id.* at § 405(f). Section 401 sets forth 13 policy goals, including, for example, "promoting full and open competition" and "eliminating fraud and waste in the procurement process." *Id.* § 401(1), (6).

<sup>757</sup> *See id.* § 408. Note that the USPS is exempt from the FAR. *See* 39 U.S.C. § 410.

<sup>758</sup> *Id.* § 412(a).

<sup>759</sup> *Id.* 413(6).

<sup>760</sup> 462 U.S. 919 (1983).

point that the FAR provides for deviation from its procedures in appropriate circumstances.<sup>761</sup>

The Procurement Policy Act applies to the procurement of:

- (1) property other than real property in being;
- (2) services, including research and development; and
- (3) construction, alteration, repair, or maintenance of real property.<sup>762</sup>

Similarly, the FAR applies to "all acquisitions,"<sup>763</sup> which are defined as "the acquiring by contract with appropriate funds of supplies<sup>764</sup> or services (including construction) by and for the use of the Federal Government through purchase or lease . . . ." <sup>765</sup> 48 C.F.R. Chapter 1 contains the FAR proper. Parts 1 through 51 of Chapter 1 contains regulations respecting the contracting process and substantive contractual provisions. Parts 52 and 53 of Chapter 1 contain specific contract language and forms, respectively.<sup>766</sup> Chapters 2 through 57 contain specific procurement regulations of various agencies and other governmental bodies. Chapters 61 and 63 contain procedural regulations for the General Services Board of Contract Appeals (the "GSBCA") and the Department of Transportation Board of Contract Appeals, respectively. Chapter 99 contains regulations of the Cost Accounting Standards Board, which has been established within the Office pursuant to section 422 of the Procurement Policy Act.<sup>767</sup>

---

<sup>761</sup> See 48 C.F.R. § 1.400 *et seq.*

<sup>762</sup> 41 U.S.C. § 405(a), (b).

<sup>763</sup> 48 C.F.R. § 1.103.

<sup>764</sup> "Supplies means all property except land or interest in land. . . ." 48 C.F.R. § 2.201.

<sup>765</sup> *Id.*

<sup>766</sup> Because these provisions and forms are adequately cross-referenced to the substantive provisions of law appearing in Chapters 1 through 51, they will not be separately discussed or quoted herein. Concerning final action by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council to amend the FAR to remove EDI barriers, *see* 59 Fed. Reg. 21318 (to be codified in 48 CFR 516; 48 CFR 552).

<sup>767</sup> 41 U.S.C. § 422.



The following analysis first discusses various features of the FAR proper (48 C.F.R. Ch. 1) as they relate to liability and protection therefrom of the federal government in connection with procurement activities generally. It concludes with a discussion of certain provisions of law concerning the acquisition and/or development of electronic services and systems,<sup>768</sup> coverage which has been specifically excluded from the scope of the Procurement Policy Act.<sup>769</sup>

## **Liability of the Federal Government**

The FAR contains few provisions on federal government liability. Those provisions are limited to liability of the federal government with respect to termination of contracts at the government's convenience or upon default; contract award protests; dispute resolution; and certain marginal situations of limited importance.

Termination of Contracts. Part 49 of the FAR governs termination of contracts generally. Subpart 49.5 mandates the inclusion of provisions in contracts that permit termination at the convenience of the government or upon default.<sup>770</sup> Upon termination, Subpart 49.1 encourages recourse to negotiated settlement procedures<sup>771</sup> and, in the failure thereof, authorizes determinations of liability by "termination contracting officers" from which the contractor may appeal.<sup>772</sup> In crafting settlements for fixed-price contracts terminated for convenience, "[t]he total amount payable to the contractor for the settlement [before deductions and credits] must not exceed the contract price less payments otherwise made or to be made under the contract."<sup>773</sup> For obvious reasons, no similar "cap" is placed on the settlement of cost-reimbursement contracts. Upon a termination for default,

---

<sup>768</sup> See 40 U.S.C. §§ 757-760.

<sup>769</sup> See 41 U.S.C. § 405(L)(1).

<sup>770</sup> See 48 C.F.R. §§ 49.501-49.505.

<sup>771</sup> See *id.* §§ 49.103(a), 49.109-1 to -6.

<sup>772</sup> *Id.* § 49.109-7. For the FAR's dispute resolution procedures, see text accompanying notes 775 - 785, *infra*.

<sup>773</sup> 48 C.F.R. § 49.207.

the government is authorized to collect liquidated damages, if any; excess repurchase costs, if any; and "other ascertainable damages."<sup>774</sup>

Protests, Disputes and Appeals. A "protest" is "a written objection by an interested party to a solicitation by an agency for offers for a proposed contract for the acquisition of supplies or services or a written objection by an interested party to a proposed award or the award of such a contract."<sup>775</sup> The ability to lodge protests is an obvious attempt to protect the integrity of the contracting process, and may become important in the context of the FCA as a result of the hyper-competitive environment the "telecommunications revolution" appears to be generating. Protests may be filed in a number of locations, including the relevant agency itself,<sup>776</sup> the GAO,<sup>777</sup> or the GSBICA.<sup>778</sup>

The filing of a protest with either the GSA or the GSBICA (General Services Board of Contract Appeals) at the expiration of any appropriation of funds has the effect of making such funds available for a period of 90 working days after the final ruling on the protest.<sup>779</sup> In addition, a protest filed with an agency, the GAO or the GSBICA precludes award of the contract in dispute unless "urgent and compelling circumstances" or the like exist.<sup>780</sup> If the GAO receives a protest *after*

---

<sup>774</sup> *Id.* §§ 49.402-7, 49.406. Collection of "contract debts" by the government is covered in Subpart 32.6, 48 C.F.R. §§ 32.600-32.617.

<sup>775</sup> 48 C.F.R. § 33.101. An "interested party" is an "actual or prospective offeror whose direct economic interest would be affected by the award of a contract or by the failure to award a contract." *Id.*

<sup>776</sup> *Id.* § 33.103. "An interested party wishing to protest . . . is encouraged to seek resolution within the agency . . . before filing a protest with the GAO [General Accounting Office] or the GSBICA [General Service Board of Contract Appeals] . . ." *Id.* § 33.102(c)(1).

<sup>777</sup> *See* 48 C.F.R. § 33.104. The GAO's own regulations respecting protests appear at 4 C.F.R. Part 21.

<sup>778</sup> *See id.* § 33.105. Protests to the GSBICA may only be made with respect to "ADP (automatic data processing) acquisitions," on which, *see* text accompanying notes 801 and 816, *infra*. An ADP acquisition protest filed with the GAO on the GSBICA precludes the filing of a protest with the other. *See id.* §§ 33.102(c)(2), (3). The GSBICA's procedural regulations appear in 48 C.F.R. ch. 61.

<sup>779</sup> *See id.* 33.102(b) (pursuant to 31 U.S.C. 1558).

<sup>780</sup> *Id.* § 33.103(b).



award of the contract, the contracting officer *must* suspend performance or terminate the contract, again in the absence of "urgent and compelling circumstances."<sup>781</sup>

Pursuant to the Contract Disputes Act of 1978,<sup>782</sup> claims for the payment of money, contract reformation, or interpretation or "other relief" are addressed by the contracting officer in the first instance.<sup>783</sup> Appeals from adverse decisions are either to the agency's Board of Contract Appeals or to the United States Claims Court.<sup>784</sup> The FAR provides for the accrual of interest on claims.<sup>785</sup>

Contractual Liability Provisions. Apart from granting the federal government general authority to enter into either fixed-price or cost-reimbursement contracts,<sup>786</sup> the FAR apparently contains but two, provisions respecting federal liability, both marginal. First, "letter" contracts, which are authorized to be used in exigent circumstances,<sup>787</sup> must contain an explicit "maximum liability" clause.<sup>788</sup> That maximum is to be "the estimated amount necessary to cover the contractor's requirements for funds before definitization [of the final contract and is not ordinarily to] exceed 50 per cent of the estimated cost of the definitive contract."<sup>789</sup>

---

<sup>781</sup> *Id.* § 33.104(c).

<sup>782</sup> 41 U.S.C. §§ 601-613.

<sup>783</sup> 48 C.F.R. § 33.206. The FAR also states that "The Government's policy is to try to resolve all contractual issues in controversy by mutual agreement at the contracting officer's level." *Id.* § 33.204.

<sup>784</sup> *See id.* § 33.211(a)(v).

<sup>785</sup> *See id.* § 33.208.

<sup>786</sup> *See, e.g., id.* § 16.101(b).

<sup>787</sup> *See id.* § 16.603-2(a).

<sup>788</sup> *Id.* § 16.603-2(d).

<sup>789</sup> *Id.*

The other special FAR provision concerns indemnification of contractors for "unusually hazardous or nuclear risks"<sup>790</sup> pursuant to Public Law 85-804.<sup>791</sup>

As in the case of indemnification of nuclear power plant operators and their contractors, the other notable instance in federal law of governmental indemnification, indemnification requires consideration of the existence and availability of insurance and other "financial protection."<sup>792</sup>

### **Protection of Federal Interests in Contracting**

In unsurprising contrast to the paucity of provisions concerning federal liability, the FAR is replete with provisions for the protection of federal interests. These provisions include protections for government property and address the carriage of insurance by contractors.

Section 45.504(a) of the FAR states:

Subject to the terms of the contract and the circumstances surrounding the particular case, the contractor may be liable for shortages, loss, damages, or destruction of Government property. The contractor may also be liable when the use or consumption of government property unreasonably exceeds the allowances provided for by the contract, the bill of material, or other appropriate criteria.<sup>793</sup>

---

<sup>790</sup> *Id.* § 50.403-1(a). Chapter 1, Part 50 of the FAR covers "Extraordinary Contractual Actions."

<sup>791</sup> Codified at 50 U.S.C. §§ 1431-1435. Public Law 85-804 confers special powers on the President concerning national defense contracting:

The President may authorize any department or agency of the Government which exercises functions in connection with the national defense . . . to enter into contracts or into amendments or modifications of contracts heretofore or hereafter made and to make advance payments thereon, without regard to other provisions of law relating to the making, performance, amendment, or modification of contracts, whenever he deems that such action would facilitate the national defense.

50 U.S.C. § 1431.

<sup>792</sup> 48 U.S.C. § 1431; *see* Section IX.B., *infra* (concerning insurance).

<sup>793</sup> 48 C.F.R. § 45.504(a).



Section 45.103 expands upon this principle: "Contractors are responsible and liable for government property in their possession, unless otherwise provided by the contract."<sup>794</sup> The single most obvious risk of "loss of or damage to government property" in the FCA context would concern certificate-related information furnished to an FCA contractor.<sup>795</sup>

With respect to insurance, it is the FAR's "policy" that:

Contractors . . . are required by law and this regulation to provide insurance for certain types of perils (e.g, workers' compensation). Insurance is mandatory also when commingling of property, type of operation, circumstances of ownership, or condition of the contract make it necessary for the protection of the Government.<sup>796</sup>

To prevent "seepage" of self-insurance costs into cost-reimbursement contracts, contractors are required to have certain types of insurance, including workers compensation, personal injury and automobile liability insurance.<sup>797</sup> However, "[p]roperty damage liability insurance shall be required only in special circumstances as determined by the agency."<sup>798</sup>

Nonetheless, the Government is not ordinarily concerned with the contractor's insurance coverage if the contract is a fixed-price contract. Examples of such circumstances include the following:

- (1) The contractor is -- or has a separate operation -- engaged principally in Government work.
- (2) Government property is involved.
- (3) The work is to be performed on a Government installation.

---

<sup>794</sup> *Id.* § 45.103(a). Instances in which "[g]enerally, Government contractors do not hold contractors liable for loss or damage to government property" include, *inter alia*, cost-reimbursement contracts and "[n]egotiated fixed-price contracts for which the contract price is not based upon (i) adequate price competition, (ii) established catalog on market prices of commercial items sold in substantial quantities to the general public, or (iii) prices set by law or regulation . . . ." *Id.* at 45.103(b)(1), (2).

<sup>795</sup> This is, of course, a separate and distinct problem from any related to unauthorized use or disclosure of such information.

<sup>796</sup> 48 C.F.R. § 28.301(b).

<sup>797</sup> *Id.* § 28.307-2.

<sup>798</sup> *Id.* § 28.307-2(b)(2).

(4) The Government elects to assume risks for which the contractor ordinarily obtains commercial insurance.<sup>799</sup>

Finally, "[a]gencies may establish risk-pooling arrangements . . . to use the services of the insurance industry for safety engineering and the handling of claims at minimum cost to the Government."<sup>800</sup>

### **Automatic Data Processing Acquisitions and the FIRMR**

As already noted, certain federal actions with respect to "automated data processing" equipment are largely excluded from the FAR and are covered by a separate statute.<sup>801</sup> In general, "[t]he [GSA] Administrator is authorized and directed to co-ordinate and provide for the economic and official purchase, lease, and maintenance of automatic data processing equipment by federal agencies."<sup>802</sup> The GSA Administrator is primarily responsible for "providing" federal agencies with automatic data processing equipment,<sup>803</sup> although this authority may be delegated to individual agencies in certain instances, including when "a senior official . . . is sufficiently independent of program responsibility."<sup>804</sup>

Pursuant to 40 U.S.C. § 759, the FIRMR covers "[t]he acquisition, management, and use of FIP resources by Federal agencies" and contracts for the delivery of FIP resources or that require the "non-incidental" use by contractors of FIP resources.<sup>805</sup> FIP resources include "[a]ny equipment or interconnected system or

---

<sup>799</sup> *Id.* § 28.206(a).

<sup>800</sup> *Id.* § 28.304.

<sup>801</sup> 40 U.S.C. § 759. Curiously, the FIRMR uses the apparently co-terminous expression "Federal information processing ('FIPS') resources." 41 C.F.R. § 201-4.001.

<sup>802</sup> 40 U.S.C. § 759(a).

<sup>803</sup> *Id.* § 759(b)(1).

<sup>804</sup> *Id.* § 759(b)(3).

<sup>805</sup> 41 C.F.R. § 201-1.002-1. There are exceptions for procurements by the Central Intelligence Agency and the Department of Defense (for activities involving, *inter alia*, "cryptologic activities related to national security"). *Id.* § 201-2(a). Nor does the FIRMR apply to radar, sonar, radio or television equipment (other than the FTS 2000 system). *See id.* § 201-2(b).



subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information - By a Federal agency, or under a contract with a Federal agency . . . ."806

Much of the FIRMR is directed toward the establishment of general guidelines for agencies to use in assessing their needs for and utilizing FIPS resources. Accordingly, this portion of the FIRMR consists largely of policy statements. However, two areas bear special mention. First, the FIRMR contemplates a system of GSA review of agency compliance.<sup>807</sup> This "audit" function accords well with the needs of the FCA.<sup>808</sup> Also, the FIRMR directs agencies to ensure a "proper level of security for all FIP resources."<sup>809</sup> Like the FAR, the FIRMR permits deviations from its provision upon prior authorization by the GSA.<sup>810</sup> Notable provisions in respect of specific contracting practices include a relatively elaborate procedure for obtaining authorization to acquire "a specific make and model specification."<sup>811</sup>

Special provisions regarding "security and privacy specifications" apply. These include explicit notification to the government of "anticipated threats and hazards"; "safeguards"; and "the test methods, procedures, criteria, and inspection system necessary to verify and monitor the operation of the safeguards."<sup>812</sup>

Interestingly, the "boilerplate" contractor liability provision, which applies "unless the contracting officer determines that a higher degree of protection is in the best interest of the government,"<sup>813</sup> expressly disclaims all express and implied warranties other than the implied warranty of merchantability and states,

---

<sup>806</sup> *Id.* § 201-4.001.

<sup>807</sup> *See id.* §§ 201-11.002, 201-22.000 *et seq.*

<sup>808</sup> *See especially* Section V.C.5.b., *supra*.

<sup>809</sup> 41 C.F.R. § 201-21.302.

<sup>810</sup> *See id.* § 201-39.104.

<sup>811</sup> *Id.* §§ 201-39.6000 *et seq.* ("Competition Requirements").

<sup>812</sup> *Id.* §§ 201-39.1001-1 *et seq.*

<sup>813</sup> *Id.* §§ 201-39.4600 *et seq.*

"In no event will the Contractor be liable to the government for consequential damages. . . ."814

The FIRMR is in a state of evolution.<sup>815</sup> Accordingly, it does not yet contain sufficient detail to provide further specific guidance in respect of contracting for FCA services. Nonetheless, it is bound to be important when and if the FCA initiative is commenced. It should be noted in closing that applicability to the FCA of the FIRMR will imply a not inconsequential role both for the GSA, which administers the FIRMR, and for NIST.<sup>816</sup>

---

814 *Id.* § 201-39.5202-6.

815 *See, e.g., id.* § 201-3.001 (future releases); *id.* § 201-3.301(b) (reserving FIRMR space for concordant agency regulations).

816 *See* Sections VII.A.4.d., *supra*. NIST plays an important role in, among other things, the security aspects of the FIRMR. *See, e.g.,* 41 C.F.R. § 201-21.303(d) (admonishing agencies, among other things, to "Consider the security and privacy guidance contained in FIRMR Bulletin C-22, OMB Circular No. A-130 Appendix III, regulations of OPM [Office of Personnel Management], and publications issued by NIST").



## **VIII. SURVEY OF, AND APPROACHES TO, TRUSTED ENTITY LIABILITY**

A trusted entity can be defined as an independent, unbiased third party that contributes to, or provides, important security assurances that enhance the admissibility, enforceability and reliability of information in electronic form. The trusted entity attributes of various private and public institutions identified below provide a rich foundation for constructing an FCA-trusted entity infrastructure. Although no one really knows precisely what is required and what will result, the need is apparent for a rationalization and harmonization of trusted entity requirements so that the developing computer-based information infrastructure will serve us well into the future.

### **A. BANKS AND FINANCIAL SERVICES**

Banks perform a variety of functions as part of their day-to-day operations that parallel or dovetail with the FCA's proposed role. These functions include, but are not limited to, the verification and execution of orders and "stop-payment" orders for the transfer of funds. They are governed in substantial part by various provisions of Articles 3, 4 and 4A of the Uniform Commercial Code (hereinafter the "U.C.C."), and internationally, where applicable, by the UNCITRAL Model Law on International Credit Transfers, which cover, respectively, negotiable instruments, bank deposits and collections and "funds transfers." These Articles, in their various incarnations, have established a number of regimes for the allocation of risk and loss. Federal law and private agreements also play an important role in banking functions.

#### **1. U.C.C. Articles 3 and 4 (Checks)<sup>817</sup>**

##### **a. Matters Related to Signature Verification**

Because certificates are used to verify digital signatures, a brief examination of analogous functions as performed by banks with respect to conventional instruments is set forth below.

---

<sup>817</sup> Articles 3 and 4 were completely amended and restated in 1990, but the revisions have not as yet been universally adopted. Unless otherwise noted, citations to specific sections will be to Revised Articles 3 and 4, which appear at 2 U.L.A. 5 and 2B U.L.A. 5 (1991), respectively. Pre-revision Articles 3 and 4, which are mentioned chiefly for comparative purposes, appear at 2 U.L.A. 209 and 2B U.L.A. 75, respectively.

Payment of Forged Checks.<sup>818</sup> U.C.C. § 4-401(a) provides that "A bank may charge against the account of a customer an item that is properly payable from the account . . . . An item is properly payable if it is authorized by the customer and is in accordance with any agreement between the customer and bank." Further, the customer will not be liable on a check unless his signature, or that of an authorized agent, appears thereon.<sup>819</sup> Accordingly, the bank may not ordinarily charge its customer for payment of a forged check. This "strict liability" for the bank obviously reflects the policy decision that, as between the bank and its customer, the one first (and thus, in theory, best) able to prevent a forgery-related loss should be the one to bear that loss.<sup>820</sup> However, this burden can shift, such as in the case of a customer "whose failure to exercise ordinary care substantially contributes to . . . the making of a forged signature"<sup>821</sup> or when the customer fails to exercise due diligence in inspecting bank statements.<sup>822</sup> Nonetheless, the customer may still succeed in shifting all or part of the burden back onto the bank on a "comparative negligence" basis.<sup>823</sup>

---

<sup>818</sup> As used herein, the expression "forged checks" refers to checks on which the "drawer's" signature has been forged or is otherwise unauthorized. Checks validly issued may also be stolen and arrive at the payor bank bearing one or more forged indorsements. These checks are described herein by the admittedly cumbersome phrase "checks bearing forged indorsements."

<sup>819</sup> See U.C.C. § 3-403(a) ("Unless otherwise provided in this Article or Article 4, an unauthorized signature is ineffective except as the signature of the unauthorized signer . . . .").

<sup>820</sup> This policy is one that exercises considerable influence. Thus, in *U.S. Fidelity and Guar. Co. v. Federal Reserve Bank*, 620 F. Supp. 361 (S.D.N.Y. 1985), *aff'd without opinion*, 786 F.2d 77 (2d Cir. 1986), the court essentially ignored Article 4's liability scheme and created a "contributory negligence" defense against claims of the depository bank in cases of "MICR" fraud.

<sup>821</sup> U.C.C. § 3-406(a).

<sup>822</sup> See *id.* U.C.C. § 4-406.

<sup>823</sup> *Id.* §§ 3-406(b), 4-406(e). The appearance of comparative negligence principles represents a substantial departure from prior law. Under former sections 3-406 and 4-406(4), the customer's negligence or lack of diligence would be wholly absolved by the bank's failure to observe "reasonable commercial standards" or lack of ordinary care, respectively.



Payment of Checks Bearing Forged Endorsements: Payment of a check that has been lost by or stolen from the payee or holder and arrives at the payor bank bearing one or more forged endorsements constitutes a conversion of the check and creates liability to its true owner.<sup>824</sup> However, because payor banks are not in the same position to inspect endorsements as they are to inspect the signatures of their own customers, this liability is typically passed "up the chain" by virtue of various transfer and presentment warranties to the entity that first accepted the check bearing the forged endorsement,<sup>825</sup> which would in the simplest case be the depository bank.<sup>826</sup>

Although liability for such losses usually falls on the customer, banks may also be liable for paying a check bearing the endorsement of an impostor or "fictitious payee" upon a failure "to exercise ordinary care" that "substantially contributes to loss . . . to the extent the failure to exercise ordinary care contributed to the loss."<sup>827</sup> The rationale here is likely that the drawer is in a reasonably good position to ensure the proper identity or even existence of persons to whom it issues checks. Thus, the payor bank is absolved of responsibility in these situations, provided it exercises "ordinary care." In addition, the bank, to the extent that it faces liability, does so only on a comparative negligence basis.<sup>828</sup>

#### **b. Failure to Observe Customer Instructions**

As has already been noted, user-requested CRLs are similar, in some respects, to "stop-payment" orders on checks.<sup>829</sup> A check on which payment has been stopped

---

<sup>824</sup> See *id.* § 3-420(a).

<sup>825</sup> See *id.* §§ 3-416(a)(1), (2) (warranties of enforceability and that all signatures are authentic upon transfer); *id.* § 4-207(a)(2) (same warranties specifically with respect to checks). Note, however, that upon presentment to the payor bank for payment, the warranty becomes only that "the warrantor has no knowledge that the signature of the purported drawer of the draft is unauthorized." *Id.* § 4-208(a)(3); see also *id.* § 3-417(a)(3) (same). It is this distinction that prevents the payor on a *forged check* from passing the loss "up the chain" to prior parties.

<sup>826</sup> The provisions noted in the previous note, of course, permit the depository bank to recover from the fraudulent indorser. However, this individual is rarely both available and solvent.

<sup>827</sup> U.C.C. § 3-404(d).

<sup>828</sup> See *id.*

<sup>829</sup> See Section V.D.2.b., *supra* (concerning issuance of CRLs by User).

is not "properly payable" pursuant to section 4-401(a) and, again, the bank may not charge its customer's account upon payment of such a check. Article 4 has imposed certain deadlines for the issuance of an effective stop-payment order,<sup>830</sup> chief among which is that the customer give the bank "a reasonable opportunity to act" prior to the occurrence of one of the events enumerated in section 4-303(a).<sup>831</sup> The customer bears the burden of proving any damages arising out of the bank's non-observance of "stop-payment" orders,<sup>832</sup> and the bank is subrogated to the payee's rights as a defense, set-off, or counterclaim.<sup>833</sup>

Section 4-401(c) establishes a similar regime for timeliness and damages with respect to post-dated checks. It should be noted, however, that the mere post-dating of a check is ineffective against the bank absent notice to the bank describing the check "with reasonable certainty."<sup>834</sup>

### c. Duty of Care and Measure of Damages

The liability of banks under the foregoing considerations is "strict" in the first instance. Banks must also use "ordinary care" in the processing, forwarding and collection of checks. As a practical matter, the exercise of "ordinary care" basically means performing various clerical and dispatching functions in a timely manner.<sup>835</sup> Article 4 does not exhaustively define "ordinary care," but it does provide certain guidelines. Specifically, compliance with Article 4 or with

---

<sup>830</sup> See U.C.C. § 4-303(a). Among these deadlines is the obvious one that occurs upon payment of an "item" (or check) in cash. *Id.* § 4-303(a)(2).

<sup>831</sup> *Id.* § 4-403(a).

<sup>832</sup> *Id.* § 4-403(c).

<sup>833</sup> See *id.* § 4-407. Although the U.C.C.'s structure and terminology appear complex, the concept is not difficult. Imagine, for example, that a buyer purchases a quantity of goods and gives the seller a check. Upon inspection, the buyer discovers defects in the goods and issues a stop-payment order that the bank fails to observe. The bank will be able to assert (is "subrogated to") the seller's right to payment in full or in part as a defense to the buyer's claim for the bank's failure to observe the order. See *id.* § 4-407 official cmt. 2.

<sup>834</sup> *Id.* § 4-401(c).

<sup>835</sup> *Id.* § 4-202(a). A classic example of the consequences that may arise as a consequence of failure to exercise ordinary care may be found in *Northpark Nat'l Bank v. Bankers Trust Co.*, 572 F. Supp. 524 (S.D.N.Y. 1983).



regulations or operating circulars of the Federal Reserve "is the exercise of ordinary care."<sup>836</sup> Moreover, compliance with clearing-house rules and a "general banking usage not disapproved by this Article, is *prima facie* the exercise of ordinary care."<sup>837</sup> Finally, "[t]he specification or approval of certain procedures by this Article is not disapproval of other procedures that may be reasonable under the circumstances."<sup>838</sup>

The measure of damages for failure to exercise ordinary care in handling a check is its amount "reduced by an amount that could not have been realized by the exercise of ordinary care."<sup>839</sup> If the bank acts in bad faith, however, the plaintiff may receive "any other damages [it] suffered as a proximate consequence."<sup>840</sup> Accordingly, in the absence of bad faith, a bank cannot expose itself to liability for negligence in an amount greater than the amount of checks it handles.<sup>841</sup>

Another source of liability, however, is that for "wrongful dishonor." Wrongful dishonor essentially constitutes a breach of the bank's contract with its customer to honor checks duly issued, such as, for example, after the bank has failed to observe a timely "stop-payment" order on a different check, or filed to credit a deposit, thus leaving the account with inadequate funds. Section 4-402(b), in contrast to earlier case law providing for automatic damages without proof of actual injury to a trader's reputation,<sup>842</sup> requires the proof of "actual damages,"

---

<sup>836</sup> U.C.C. § 4-103(c) (emphasis added).

<sup>837</sup> *Id.*

<sup>838</sup> *Id.* § 4-103(d).

<sup>839</sup> *Id.* § 4-103(e).

<sup>840</sup> *Id.*; see also *Casco Bank & Trust Co. v. Bank of N.Y.*, 584 F. Supp. 763 (D. Me. 1984).

<sup>841</sup> However, U.C.C. § 4-103(a) permits variation by agreement so long as the bank does not disclaim its "responsibility for its lack of good faith or failure to exercise ordinary care or limit the measure of damages for the lack or failure." Variation by agreement is further considered in Section IX.D.2.b., *supra*.

<sup>842</sup> See U.C.C. § 4-402 official cmt. 1 (discussing abrogation of "the so-called 'trader' rule"). The rule appears to have been similar, and indeed may have been founded upon, the "libel *per se*" doctrine. See, e.g., RESTATEMENT OF TORTS (SECOND), *supra* note 244, §§ 569-570. One of the actions that could give rise to liability for damages without proof was to state falsely that a merchant was or had been a bankrupt. *Id.* § 573. This kind of statement presented problems in that until the middle of the nineteenth century, bankruptcy law was formally considered

which "may include damages for an arrest or prosecution of the customer or other consequential damages."<sup>843</sup>

#### **d. Specifically Electronic or Computer-Related Matters**

The 1990 revisions to Article 4 added several provisions that reflect changes in technology since its original 1952 promulgation. Article 4 now provides for electronic presentment of checks, for example.<sup>844</sup> More relevant to the concerns of this Report, however, are an exculpatory provision respecting delay caused by interruption of computer facilities, provided the bank exercises "such diligence as the circumstances require"<sup>845</sup> and a new section establishing warranties of accurate electronic presentment and encoding of information for automated check processing.<sup>846</sup>

#### **2. U.C.C. Article 4A (Funds Transfers)**

Article 4A deals with "funds transfers," specifically "wholesale wire transfers,"<sup>847</sup> which are often, but need not be, effected by electronic communications.<sup>848</sup> The drafters of

---

solely as a device for the collection of debts. Actions, which were "semi-criminal" in nature, could only be commenced by creditors against persons in trade. Accordingly, to state that a person in trade was not paying his bills in a timely fashion was to expose that person to consequences different from those that would pertain to a person not in trade.

<sup>843</sup> U.C.C. § 4-402(b).

<sup>844</sup> *See id.* § 4-110.

<sup>845</sup> *See id.* § 4-109(b).

<sup>846</sup> *Id.* § 4-209. The Federal Reserve proposes to authorize Reserve Banks to engage in electronic processing pursuant to an operating circular/agreement respecting "Electronic Check Presentment Services." A draft dated June 30, 1993 was circulated at the American Bar Association's Annual Meeting in New York City, August 1993. Sections 10-17 thereof include broad exculpatory and indemnification provisions running in favor of the Reserve Bank(s).

<sup>847</sup> Prefatory Note to Article 4A, 28 U.L.A. 455, 457 (1991).

<sup>848</sup> Article 4A defines "funds transfer" as "the series of transactions . . . made for the purpose of making payment to the beneficiary of the order." U.C.C. § 4A-104(a). Apart from purely financial settlement matters, "funds transfers" consist



Article 4A recognized certain of the problems associated with the extensive use of non-written, legally operative communications and accordingly defined and conferred formal significance upon "security procedures." Accordingly, Article 4A provides a useful model for dealing with the allocation of risk for substantially instantaneous transactions of potentially enormous value.

#### a. The Role of Security Procedures

An important facet of Article 4A's liability regime is its reliance upon "security procedures." Section 4A-201 defines "security procedure" to mean "a procedure established by agreement of a customer and a receiving bank" that is implemented for the purpose of (i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication."<sup>849</sup> Section 4A-201's illustrative list of security procedures features arguably would tend to support the use of public key cryptographic security mechanisms, although, of course, such technology was not specifically contemplated.<sup>850</sup> Interestingly, to be effective under Article 4A, "security procedures" go beyond the scope of banks' duties under Article 4: "Comparison of a signature on a payment order or comparison with an authorized specimen signature of the customer is not by itself a security procedure."<sup>851</sup>

In general, Article 4A places considerable responsibility on customers to protect the integrity of security procedures agreed upon with banks. Thus, a payment order will be "effective" as the order of a customer, even if it is in fact unauthorized by the customer, if a security procedure is in place; and it is "commercially reasonable and the payment order is accepted in good faith and in

---

principally of "payment orders" from the "originator" (or payor) to the "originator's bank" and thence, with or without the use of "intermediary banks," to the "beneficiary's bank" and ultimately to the "beneficiary." *Id.* §§ 4A-103, 4A-104. A "payment order" may be "transmitted orally, electronically, or in writing." *Id.* § 4A-103 (a)(1).

<sup>849</sup> *Id.* § 4A-201.

<sup>850</sup> "A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices." *Id.*

<sup>851</sup> *Id.*

compliance with the security procedure."<sup>852</sup> Thus, if a bank accepts a payment order in compliance with the foregoing requirements, it will be entitled to collect the amount of a fraudulent order from the "sender,"<sup>853</sup> subject to two caveats. First, the bank may contractually limit its right to enforce so-called "verified" (but unauthorized) payment orders. Second, the customer may resist liability for the unauthorized order if it can prove that the order was "*not* caused, directly or indirectly" by a person entrusted with payment order/security procedure duties by the customer or who obtained access to transmitting facilities or "information facilitating breach of the security procedure" from "a source controlled by the customer and without authority of the receiving bank."<sup>854</sup> The point of this provision is to make the customer strictly liable for misuse of security procedures unless the customer can *prove*, in essence, that any compromise of security did not originate with the customer, its personnel, or its equipment. In the eyes of the Article 4A draftsmen, compromise of security procedures must arise either with the customer or with the bank.<sup>855</sup> If the customer can prove a total absence of involvement on its part, then the bank will bear the loss. When the order is not authorized, effective, or enforceable, the bank must return the funds, with interest, to the sender.<sup>856</sup> Effectively, then, a receiving bank is *strictly liable* for unauthorized orders if: 1) no security procedure is in place; 2) the bank fails to

---

<sup>852</sup> *Id.* § 4A-202(b). Interestingly, the "commercial reasonableness" of a given security procedure is a "question of law." *Id.* § 4A-202(c). The Official Comments state that this designation is appropriate because procedures are likely to become standardized and "a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers." *Id.* § 4A-203 cmt. 4. It should be noted, however, that granting commercial reasonableness "question of law" status will not reduce the need for plenary trials, because the bank must still prove good faith and compliance. Incidentally, most courts have taken the mandate of U.C.C. § 9-504(3) that sales of collateral be "commercially reasonable" to present an *issue of fact*. See, e.g., *General Elec. Capital Corp. v. Vashi*, 480 N.W.2d 880 (Iowa 1992); *U.S. Roofing v. Credit Alliance Corp.*, 279 Cal. Rptr. 533 (1991).

<sup>853</sup> U.C.C. § 4A-402(c).

<sup>854</sup> *Id.* § 4A-203 (emphasis added).

<sup>855</sup> *Id.* § 4A-203 cmt. 5.

<sup>856</sup> See *id.* § 4A-204(a). Somewhat illogically, however, the sender forfeits *all* interest if it fails to exercise ordinary care in inspecting funds transfer reports and reporting unauthorized transfers to the bank. See *id.* A more sensible rule might have been to cease the accrual of interest only as of the time the sender could reasonably have taken action.



observe a security procedure that is in place; or 3) the customer can prove it is not the source of any compromise of the security procedure.

Different considerations arise when the parties rely on a certificate issued by a third party FCA. Under Article 4A as it presently exists, the bank would suffer the consequences of a compromise of security on the part of the FCA (assuming that the customer has made the requisite showings under section 4A-203(1)(b)).

Moreover, the legal consequences of the use or non-use of security procedures depend on the security procedure's goals: verification of identity and/or detection of error.<sup>857</sup> To the extent FCA-generated certificates are used or relied upon for different or additional goals, additional liability provisions will need to be formulated to address them adequately.

## **b. Errors and Delays**

Article 4A treats a funds transfer as a series of messages from the originator to the beneficiary's bank that ultimately results in funds being made available to the beneficiary. The paradigm transaction would involve the delivery of a payment order to the originator's bank, which passes that message accurately and without delay either to the beneficiary's bank or to an intermediate bank, which would in turn pass the message accurately, again, either to the beneficiary's bank or to yet another intermediate bank, and so forth until the beneficiary's bank delivers the funds to the beneficiary.<sup>858</sup> The incrementalized structure of funds transfers under Article 4A gives rise to two sets of problems: "sender" errors and "execution" errors.

### **"Sender" Errors**

"Sender" error arises when the originator mistakenly directs payment to an unintended person or in an excessive amount. It can also arise when any sender mistakenly transmits a duplicate payment order or attempts to direct an order to a non-existent, unidentifiable or ambiguous receiving bank or beneficiary.

Security procedures play an important part in preventing errors respecting payment orders for an unintended beneficiary, payment orders in an excessive

---

<sup>857</sup> See *id.* § 4A-201. Sections 4A-202 through 204 address identification issues. Section 4A-205 concerns the use or non-use of security procedures for the detection of errors and is discussed in the text accompanying notes 860-862, *infra*.

<sup>858</sup> See generally *id.* art. 4A prefatory note.

amount,<sup>859</sup> and duplicate payment orders.<sup>860</sup> Generally, an originator or other sender bears responsibility for these errors. However, if the originator or sender utilizes a "security procedure for the detection of error" which is ignored by the receiving bank, and the originator or sender proves that compliance with the security procedures by the receiving bank would have detected the error, the originator or sender is only responsible for the correct amount, and the receiving bank will be left to pursue the beneficiary for any excess funds paid.<sup>861</sup> Nonetheless, if the originator or sender fails to notify the receiving bank of the error within a reasonable time of notification, it will be liable to the receiving bank for any resulting risk.<sup>862</sup>

Sections 4A-207 and 4A-208 address "misdescription" of beneficiaries and receiving banks, respectively. When the beneficiary is non-existent or unidentifiable, the beneficiary's bank cannot accept the payment order.<sup>863</sup> When the payment order directs payment to an account bearing a name and number identifying different persons, the beneficiary's bank may rely on the account number alone, provided it does not notice the discrepancy.<sup>864</sup> If such reliance results in payment to a person "not entitled to receive payment," either the originator or the originator's bank will nonetheless be responsible for paying the amount of the order and may seek recovery from the mistaken beneficiary.<sup>865</sup> On the other hand, if the beneficiary's bank notices a discrepancy between name and number, or if it relies on the name alone, it does so at its own risk.<sup>866</sup>

---

<sup>859</sup> Presumably, the "remedy" for an originator's payment order in an inadequate amount is to transmit a supplemental payment order.

<sup>860</sup> See generally U.C.C. § 4A-205.

<sup>861</sup> *Id.* § 4A-205(a).

<sup>862</sup> See *id.* § 4A-205(b). The originator/sender's liability, however, cannot exceed the amount of its order. See *id.*

<sup>863</sup> *Id.* § 4A-207(a).

<sup>864</sup> *Id.* § 4A-207(b)(1). The beneficiary's bank, moreover, has no duty to check for such discrepancies. See *id.* However, the originator must have been on notice of this arrangement prior to acceptance of the payment order in order for the bank to invoke this rule.

<sup>865</sup> *Id.* § 4A-207(c), (d).

<sup>866</sup> See *id.* § 4A-207(b)(2).



Similar, but not identical, rules pertain when a receiving bank has been "misdescribed." If it has been identified only by number, the receiving bank may rely on that number, and it "need not determine whether the number identifies a bank."<sup>867</sup> If the name and number identify different institutions, the receiving bank may always rely on the name alone,<sup>868</sup> and in certain circumstances, on the number alone,<sup>869</sup> provided it does not notice the discrepancy. If it transmits a payment order to one or the other institution with knowledge of a discrepancy, it does so at its own risk.<sup>870</sup>

A final source of "sender" error arises from the use of a "funds-transfer system or other third-party communication system for transmittal."<sup>871</sup> Such an organization is deemed an agent of the sender, and its errors bind the sender.<sup>872</sup>

### "Execution" Error

When a receiving bank undertakes to accept and execute a payment order,<sup>873</sup> it obligates itself to "issue, on the execution date, a payment order complying with the sender's order and to follow the sender's institution's orders concerning (i) any intermediary banks or funds-transfer system to be used . . . or (ii) the means by which payment orders are to be transmitted."<sup>874</sup> If the sender does not specify these latter two points, the receiving bank has substantial discretion with respect to the choice of "means," provided they are reasonable,<sup>875</sup> and with respect to the

---

<sup>867</sup> *Id.* § 4A-208(a)(1). Pursuant to section 4A-208(a)(2), the receiving bank may also look to its sender for its "loss and expenses."

<sup>868</sup> *See id.* § 4A-208(b)(3).

<sup>869</sup> *See id.* § 4A-208(b)(1), (2).

<sup>870</sup> *See id.* § 4A-208(b)(4).

<sup>871</sup> *Id.* § 4A-206(a).

<sup>872</sup> *Id.*

<sup>873</sup> Absent express agreement to the contrary, no bank is under any duty to accept payment orders. *See id.* § 4A-212.

<sup>874</sup> *Id.* § 4A-302(a)(1).

<sup>875</sup> *Id.* § 4A-302 (a)(2), (c).

choice of payment system or intermediary bank, provided it exercises ordinary care in the selection of the intermediary bank.<sup>876</sup>

The typical execution error is to receive an accurate payment order and to transmit an inaccurate version. When a receiving bank transmits an excessive payment order or a duplicate payment order, it may only claim payment from the sender in the correct amount, and must collect any surplus funds from the beneficiary.<sup>877</sup> If the receiving bank makes an execution error resulting in payment to an incorrect "beneficiary," neither the sender nor any previous sender need pay its respective payment order, and, again, the receiving bank is left to collect the wrongful payment on its own account.<sup>878</sup>

In terms of damages for "execution" errors, "[t]he judgment of the drafters of Article 4A that banks should not be liable for consequential damages represents the most fundamental policy decision underlying the whole article."<sup>879</sup>

---

<sup>876</sup> *Id.* § 4A-302(b). In the event an intermediary bank goes into receivership or otherwise stops payment, the party choosing that intermediary bank will often suffer the consequences. *See, e.g., id.* § 4A-402(e).

<sup>877</sup> *Id.* § 4A-303(a).

<sup>878</sup> *Id.* § 4A-303(c). Section 4A-303(b) addresses the relatively less harmful situation in which a payment order of insufficient amount is executed.

<sup>879</sup> R. GOTTLIEB, ET AL., U.C.C. ARTICLE 4A: A PRACTICAL GUIDE FOR BANKERS AND BANK COUNSEL 52 (1991); *see also* notes 332-340 (addressing *Evra Corp. V. Swiss Bank Corp.*, 673 F.2d 951 (7th Cir. 1982), which is discussed extensively in U.C.C. § 4A-305, cmt. 2). The drafters of Article 4A, in fact, rejected *Evra* unambiguously:

If *Evra* means that consequential damages can be imposed if the culpable bank has notice of particular circumstances giving rise to the damages, it does not provide an acceptable solution to the problem of bank liability for consequential damages. In the typical case transmission of the payment order is made electronically. Personnel of the receiving bank that process payment orders are not the appropriate people to evaluate the risk of liability for consequential damages in relation to the price charged for the wire transfer service. Even if notice is received by higher level management personnel who could make an appropriate decision whether the risk is justified by the price, liability based on notice would require evaluation of payment orders on an individual basis. This kind of evaluation is inconsistent with the high-speed, low-price, mechanical nature of the processing system that characterizes wire transfers. Moreover, in *Evra* the culpable bank was an intermediary bank with which the originator did not deal. Notice to the originator's



Accordingly, consequential damages are unavailable for delay or non-completion of the funds transfers, for failure to use the intermediary bank designated by the originator; issuance of a non-complying payment order; or for failure to accept a payment order (when the bank has so obligated itself by agreement) absent "express written agreement of the receiving bank."<sup>880</sup> Consequential damages *are* available to the beneficiary, however, when the beneficiary's bank obligates itself to pay the beneficiary by accepting a payment order and the bank "refuses to pay after demand by the beneficiary and receipt of notice of particular circumstances . . . unless the bank proves . . . a reasonable doubt concerning the right of the beneficiary to payment."<sup>881</sup>

---

bank would not bind the intermediary bank, and it seems impractical for the originator's bank to convey notice of this kind to intermediary banks in the funds transfer. The success of the wholesale wire transfer industry has largely been based on its ability to effect payment at low cost and great speed. Both of these essential aspects of the modern wire transfer system would be adversely affected by a rule that imposed on banks liability for consequential damages. A banking industry amicus brief in *Evra* stated: 'Whether banks can continue to make EFT services available on a widespread basis, by charging reasonable rates, depends on whether they can do so without incurring unlimited consequential risks. Certainly, no bank would handle for \$3.25 a transaction entailing potential liability in the millions of dollars.'

As the court in *Evra* also noted, the originator of the funds transfer is in the best position to evaluate the risk that a funds transfer will not be made on time and to manage that risk by issuing a payment order in time to allow monitoring of the transaction. The originator, by asking the beneficiary, can quickly determine if the funds transfer has been completed. If the originator has sent the payment order at a time that allows a reasonable margin for correcting errors, no loss is likely to result if the transaction is monitored. The other published cases on this issue reach the *Evra* result. *Central Coordinates, Inc. v. Morgan Guar. Trust Co.*, 40 U.C.C. Rep. Serv. 1340 (N.Y. Sup. Ct. 1985), and *Gatoil (U.S.A.), Inc. v. Forest Hill State Bank*, 1 U.C.C. Rep. Serv. 2d 171 (D. Md. 1986). An originator's bank might be willing to assume additional responsibilities and incur additional liability in exchange for a higher fee.

U.C.C. § 4A-305 cmt. 2.

<sup>880</sup> *Id.* § 4A-305.

<sup>881</sup> *Id.* § 4A-404 (a).

Thus, Article 4A confines liability for execution error to items such as expenses incurred and interest losses in ordinary cases.<sup>882</sup> Additionally, attorney's fees are available if a demand for compensation under section 4A-305 is made prior to commencing legal proceedings.<sup>883</sup>

---

<sup>882</sup> *See id.* § 4A-305(a), (b), (d). A related problem is delay in giving notice of a *rejected* payment order when the rejecting bank has funds of the sending bank immediately available to it. Here, too, damages are limited to interest. *See id.* §§ 4A-209(b)(3), -210(b).

<sup>883</sup> *See id.* § 4A-305(e).



### 3. AUTOMATED CLEARING HOUSES

Automated clearing houses provide both a physical and a conceptual forum for the computer-based exchange of payment orders and the provision of settlement functions among financial institutions. They are typically voluntary, private associations among institutions at the local or regional level. Since 1972, "automated" clearing houses (each, an "ACH") dealing in "paperless" transactions have proliferated.<sup>884</sup> Because ACHs provide *trusted entity* functions with respect to the communication and execution of electronic payment orders, the principles of risk allocation that have been embodied in NACHA's Operating Rules<sup>885</sup> also bear relevance to the present inquiry.<sup>886</sup> NACHA itself may also provide important institutional and administrative mechanisms to support commercial and quasi-governmental certification authorities.<sup>887</sup>

"Direct deposit" for payroll and the automated payment of bills are perhaps the most familiar applications of ACH functions. The NACHA "Operating Rules" (the "ACH Rules") govern relations among constituents in participating ACHs. Those constituents include "Originators" of payment orders or "entries";<sup>888</sup>

---

<sup>884</sup> NATIONAL AUTOMATED CLEARING HOUSE ASS'N ("NACHA"), OPERATING GUIDELINES 1, *reprinted in* ACH RULES, at OG 1 (1992).

<sup>885</sup> NACHA, OPERATING RULES, *reprinted in* ACH RULES, *supra* note 884, at OR i *et seq.*

<sup>886</sup> *See generally* ELECTRONIC CONTRACTING, *supra* note 2, at 262-70.

<sup>887</sup> NACHA has either developed or promoted a number of policies, structures, and approaches to trust and information security. For example, the NACHA Board of Directors has adopted policy statements on Data Security (1986) and the "All-Electronic ACH Network" (1990). *See* ACH RULES, *supra* note 884, at OR xv-xvii. These policy statements encourage participants to employ data security techniques in accordance with ANSI standards for authentication and key management and to develop an "all-electronic" network, which is defined as "[o]ne in which the ACH Operator and each of its participating institutions and/or servicers interface with each other via a secured telecommunications link for *all* ACH related activity. . . ." *Id.*

<sup>888</sup> "Entries" may be *debit* entries or *credit* entries. Debit entries constitute orders to deduct funds from the *Receiver's* account and credit entries orders to credit the Receiver's account. Credit entries are basically traditional wire transfers and are governed by the Electronic Funds Transfer Act ("EFTA") (codified as amended at 15 U.S.C. §§ 1601 *et seq.*) if they involve an individual consumer's non-business account and by U.C.C. Art. 4A if not. *See* 15 U.S.C. §§ 1693 ("Findings and purpose"), 1693a ("Definitions"); U.C.C. §§ 4A-102 (applicability to "funds

"Originating Depository Financial Institutions" ("ODFIs"), who are ACH members and act as Originators' links to the payment system; ACH Operators, one or more of which operate an ACH on a day-to-day basis; Receiving Depository Financial Institutions ("RDFIs"); and Receivers.

The ACH Rules, similar to U.C.C. Articles 3 and 4, derive a considerable part of their liability-ordering system from the imposition of liability for breach of warranties arising by operation of law upon the taking of certain actions. The ACH Rules impose warranties and liability for damages both on ODFIs and RDFIs. The warranties of an RDFI are extremely limited and require little discussion.<sup>889</sup>

By contrast, an ODFI warrants a series of facts to each RDFI, ACH Operator and Association. These include that both the Originator *and* the Receiver have authorized the delivery of entries on the Originator's behalf to the Receiver and/or its account; that the entry is timely and, if a debit entry, that the underlying obligation has matured; that notice of various legal consequences has been given by the ODFI and the RDFI; that authorizations have neither been revoked nor terminated by operation of law; that the Originator has complied with the ANSI X9.8 standards for PIN Management and Security; and that the ODFI's entry contains an accurate account number for the Receiver and the information necessary for the RDFI to report entries to the Receiver.<sup>890</sup>

---

transfers"), 4A-108 (exclusions of transfers covered even in part by EFTA). The ACH Rules occasionally provide for explicitly differing treatments depending on the underlying law governing a particular credit entry. *See, e.g.*, ACH RULES, *supra* note 884, Rule 5.1.2 ("Requirements of Returns").

<sup>889</sup> "Each RDFI shall be deemed to warrant to each ODFI, ACH Operator, and Association that it has the power under applicable law to receive entries as provided in these rules and to comply with the requirements contained in these rules. . . ." ACH RULES, *supra* note 884, Rule 4.2; *see also id.* Rule 5.3.1. (RDFI's warranty of accuracy in notification of change in destination of entries, such as when a Receiver decides to use a different account).

<sup>890</sup> *See id.* Rule 2.2.1. ACH Rule 2.2.1.8., dealing with payments of "pension, annuity or other benefit payments" pursuant to Rule 4.7, imposes a generalized warranty of accuracy, however. *Id.* Rule 2.2.1.8(a). Special rules apply with respect to the RDFI's liability for such payments. ACH Rules 4.7.1 and 4.7.2. Such liability is limited to the lesser of the amount of the mistaken payment or the balance in the Receiver's account at the time the ODFI notifies the RDFI of the error. *See id.* Rule 4.7.1. Any claim of an ODFI or Originator is subordinate to repayment claims of the federal government pursuant to 31 C.F.R. Part 210 ("Federal Payments Through Financial Institutions By the Automated Clearing House System"), and the ODFI is liable for disgorgement of amounts paid in contravention of the government's priority. *See id.* *See also* Sinclair Oil Corp. v. Sylvan State Bank, 869



Damages for breach of warranty on the part of ODFIs include blanket indemnification for "any and all claims, demands, loss, liability or expense, including attorney's fees and costs, resulting directly or indirectly from the breach of such warranty . . . ." <sup>891</sup>

It was noted above that the ODFI ordinarily warrants the accuracy of the Receiver's account number. Other errors give rise to new rights and obligations on the part of various parties.<sup>892</sup> If an Originator, ODFI, or ACH Operator erroneously sends a duplicate entry, it may send a "reversing file" to correct the error.<sup>893</sup> The sending of a reversing file by any of these entities creates a broad indemnification liability to subsequent parties, except that the ODFI bears the potential liability on behalf of its Originator.<sup>894</sup> Alternatively, an ODFI may request that an RDFI return or adjust an erroneous entry: "[a]n ODFI making such a request indemnifies an RDFI from and against any and all claims . . . ." <sup>895</sup> *Per diem* compensation for erroneous entries that are reversed or that are returned or adjusted at the request of the ODFI is based on the federal funds rate.<sup>896</sup>

The foregoing scheme places a heavy burden on ODFIs. They are made responsible for matters over which they have limited knowledge or control, such as the existence of proper Originator and Receiver authorizations, and the giving of various notices by the RDFI. Although this allocation scheme may seem arbitrary at best, it might be justified by considering the ODFI, the (possibly unsophisticated) Originator's member-link to the ACH, as the entity with the

---

P.2d 675 (Kan. 1994) (deciding that the ACH RULES and Fed. Reserve Bank Operating Letter No. 12 modify the provisions of U.C.C. Article 4).

<sup>891</sup> *Id.* Rule 2.2.2.

<sup>892</sup> There is no right to "recall" an entry once it has reached the ACH Operator. *Id.* Rule 7.1.

<sup>893</sup> *Id.* Rule 2.4.

<sup>894</sup> *See id.* Rule 2.4.5.

<sup>895</sup> *Id.* Rule 7.2.

<sup>896</sup> *See id.* Rules 10.8, 10.9. Interestingly, the ACH Rules contain the following statement respecting compensation: "Not every possible situation involving a claim for compensation is explicitly addressed. When a meritorious claim for compensation not covered by these rules is identified, it is expected that the [participants] involved will settle such claim so that [unjust enrichment and injury are avoided]." *Id.* Rule 10.2.

"last clear chance" of ensuring the minimum existence of problems and errors before commencing a series of virtually instantaneous messages bearing financial and legal import.

However, NACHA Operating Guidelines require the ODFI to execute an agreement with the Originator "which, at a minimum, binds the Originator to the ACH Operating Rules."<sup>897</sup> This agreement offers the ODFI an opportunity to shift the broad responsibilities assigned it by the ACH Rules to the Originator to a substantial degree.<sup>898</sup>

The Sample Agreement shifts responsibility for most mishaps onto the Originator. It limits the ODFI's liability to instances involving its own negligence<sup>899</sup> and disclaims agency status of subsequent parties.<sup>900</sup> "In no event shall [the ODFI] be liable for any consequential, special, punitive or indirect loss or damage."<sup>901</sup> Moreover, the Originator is held strictly liable for misuse of any security procedure in effect, except that when holographic signatures are employed, the ODFI must "on the basis of . . . comparison, believe [ ] the signature . . . to be that of such authorized representative."<sup>902</sup>

---

<sup>897</sup> *Id.* at OG 13. A sample ODFI-Originator Agreement [hereinafter SAMPLE AGREEMENT] appears in the ACH Rules at OG 16-21. It should be noted, however, that the Sample Agreement is not "decreed" and that the issues treated therein are a matter of contract.

<sup>898</sup> The Sample Agreement, for example, shifts many of the risks imposed on the ODFI by the Operating Rules to the Originator. Chief among these are that the Originator has no right to cancel or amend an entry after receipt by the ODFI and that the Originator represents the existence of the Receiver's authorization and agrees to indemnify the ODFI for related losses. SAMPLE AGREEMENT, *supra* note 897, ¶¶ 6, 11; *cf.* text accompanying notes 891-896, *supra*.

<sup>899</sup> Interestingly, the SAMPLE AGREEMENT is silent respecting liability for willful misconduct.

<sup>900</sup> SAMPLE AGREEMENT, *supra* note 897, ¶ 12(a). Paragraph 12(a) further provides for indemnification of the ODFI for any claims based on its alleged status as a principal. *See id.*

<sup>901</sup> *Id.* ¶ 12(b).

<sup>902</sup> *Id.* ¶ 13(a). Paragraphs 12(b) and 13(a) epitomize a fundamental split in payment systems law. For paper-based, signature-oriented processing systems, the bank is typically held to a certain concrete duty of care to inspect signatures and the like and may be held liable for consequential damages for losses caused by its failure to do so. In electronic systems, the introduction of non-signature-oriented



Article 12 of the ACH Rules sets forth certain rules respecting liability of the ACH itself to its members and to other ACHs. Pursuant to Rule 12.3, the ACH is liable for the negligence and willful misconduct of itself and of each ACH Operator. For negligence or willful misconduct in connection with a "credit" entry, damages are limited to those that are "attributable directly or indirectly" to the conduct at issue; consequential damages are precluded, "even if such consequences were foreseeable at the time of such conduct."<sup>903</sup> For "debit" entries, damages are ordinarily measured by the amount of the entry, less damages that could not have been avoided absent the negligence or willful misconduct. In a case of willful misconduct, damages may also include "direct[]" and immediate[]" losses. Consequential damages are again precluded however.<sup>904</sup> Finally, negligence or willful misconduct in the context of the giving of various notices give rise to damages only in the amount of any fee that had been collected in connection with the notice.<sup>905</sup>

In terms of scope of liability, the ACH Rules provide that ACH Operators are answerable for the negligence and willful misconduct of their employees.<sup>906</sup> However, the ACH Rules attempt to insulate other parties from liability for the negligence or willful misconduct of ACH Operators and their employees by providing for agency status on the part of ACH Operators with respect to ODFIs and RDFIs.<sup>907</sup>

ACHs are also deemed to make certain warranties and representations to other ACHs and their members. These include representations as to the existence of

---

security procedures has resulted in almost absolute liability for the customer for their mis-use and, when the bank bears responsibility. Consequential damages are precluded. This development amounts to the creation of a fictional "assumption of the risk" on the part of customers who elect to conduct transactions using media that consist of a series of mechanical operations and that require little or no human intervention.

<sup>903</sup> ACH RULES, *supra* note 884, Rule 12.3.

<sup>904</sup> *Id.*

<sup>905</sup> *See id.*

<sup>906</sup> *See id.*

<sup>907</sup> *See id.* ACH Rule 12.6.

authorization on the part of ODFIs and RDFIs to transmit or receive entries.<sup>908</sup> Rule 12.1.4 further provides for a warranty to the effect that ACH Operators have agreed to indemnify the ACH for their negligence and willful misconduct.<sup>909</sup> Damages for breach of the foregoing warranties include indemnification "from and against any and all claims, demands, loss, liability or expenses, including attorneys' fees and costs, resulting directly or indirectly from such breach."<sup>910</sup>

#### 4. The New York Clearing House Association and CHIPS

The New York Clearing House Association (NYCHA) offers the Clearing House Interbank Payments System ("CHIPS"), which is "an on-line, real-time electronic payment system that transfers funds and settles transactions in U.S. dollars. . . . It is the central clearing system in the United States for international transactions, handling over 95% of all dollar payments [close to U.S. \$ 1 trillion per day] moving between countries around the world."<sup>911</sup>

The Rules governing the Clearing House Interbank Payments System (the "CHIPS Rules"), together with certain provisions of the NYCHA Constitution establish several liability apportionment schemes that may be relevant to various FCA architectures.

---

<sup>908</sup> See *id.* Rules 12.1, 12.2. Note that ACHs are protected from breaches of their warranties by the warranties of the ODFIs, which in turn may be protected by Originator warranties. See text accompanying notes 889-890, *supra*.

<sup>909</sup> The efficacy of this warranty is vitiated to a substantial degree by the proviso, "[except] to the extent such contract [between the ACH and ACH Operators] provide that the ACH Operator . . . shall not be liable to the [ACH]." ACH RULES, *supra* note 884, Rule 12.1.4(1).

<sup>910</sup> *Id.* Rule 12.1.5.

<sup>911</sup> NYCHA Informational Brochure on CHIPS 1 (1991).



At the "global" level, the NYCHA Constitution disclaims liability as follows:

The Association shall be in no way responsible in regard to the exchanges between the members, nor in regard to the balances resulting therefrom. Should any loss occur as the result of the custody or handling of checks or collection items by the President or any other officer or employee of the Association (other than as a result of the failure of any member), it shall be borne and paid by the members pro rata according to the average amount which each shall have sent to the Clearing House for the preceding year.<sup>912</sup>

To bolster its integrity, the NYCHA Constitution permits the NYCHA to:

establish and/or maintain a Department of Examination of the Clearing House and prescribe the rules and regulations under which it is to be conducted; may examine, or cause to be examined, any member whenever deemed by it to be in the interest of the Association and, in its discretion, may require any member to protect its balances resulting from the exchanges by depositing with the [Clearing House] Committee satisfactory security or otherwise.

The Clearing House Committee may, if it deems it advisable in the interests of the Association, and unless prohibited by law or regulation of an authority with appropriate jurisdiction, inspect the reports of examination of any member made by the Board of Directors of such member, any bank supervisory authority, or any other governmental or public authority charged with the duty of making such examination. Each member shall submit to the President of the Clearing House at least once in each year . . . a copy of an audit report of such member covering such member's immediately preceding fiscal year . . . .<sup>913</sup>

As a result of their choice of law provision,<sup>914</sup> the CHIPS Rules are supplemental to Article 4A of the Uniform Commercial Code.<sup>915</sup> In this sense, the CHIPS Rules "go beyond" Article 4A and seek to establish a regime for the sharing of risk of bank failure and other mishaps among participants. The most interesting facet of this regime from the standpoint of FCA operations is its attempt to apportion liability among participants based on the nature and extent of possible losses, as defined by positive law.

---

<sup>912</sup> NYCHA Constitution, art. II, § 1 (as amended through Oct. 24, 1990). Given that this provision was amended on October 25, 1989, almost 20 years after the commencement of CHIPS operations, it is unclear whether the reference to "checks or collection items" refers to messages directed through CHIPS.

<sup>913</sup> NYCHA Constitution, art. VI, § 4.C.

<sup>914</sup> "The right and obligations of Participants . . . shall be governed by the Law of the State of New York . . ." CHIPS Rule 3.

<sup>915</sup> New York has adopted Article 4A. See 1990 N.Y. LAWS, ch. 208, § 1. Article 4A is discussed at Section VIII.A.2., *supra*.

Given CHIPS' daily transmission volume, the prospect of a failure to settle on the part of a sufficiently important participant leads to domino-effect scenarios of global financial collapse.<sup>916</sup> Accordingly, a chief focus of the CHIPS Rules is to assure settlement on a daily basis. This is accomplished by a complex set of features designed to apportion a failing bank's net liability to CHIPS among remaining participants ratably according to the degree to which each participant "contributed" to the loss by setting higher or lower limits, relative to those set by other participants, on the debit position it would permit the failed participant to hold with it.<sup>917</sup> The maximum liability for each participant is five percent of the highest "bilateral limit" it issued that day.<sup>918</sup> Each participant's obligation to fund an Additional Settlement Obligation is collateralized by federal securities in the amount of its maximum liability therefor.<sup>919</sup> Because CHIPS will not permit an individual participant's net liability to the system to exceed five percent of the total of the bilateral limits granted to it,<sup>920</sup> the laws of mathematics and the pragmatics of collection ensure that CHIPS will be able to settle even upon failure of its largest participant. The failure of more than one participant is likely to be recoverable as well, but this is not a matter of mathematical certainty.<sup>921</sup> In the event settlement does not occur, the NYCHA Clearing House Committee, "after consultation with such parties as it deems appropriate, shall have the authority to take such action as it deems appropriate . . ."<sup>922</sup> The final result under the

---

<sup>916</sup> See, e.g., Humphrey, *Payments Finality and Risk of Settlement Failure*, in A. SAUNDERS & L. WHITE, *TECHNOLOGY AND THE REGULATION OF FINANCIAL MARKETS* 97 (1986).

<sup>917</sup> CHIPS Rules 13(e), (h) (instituting "Additional Settlement Obligation" for non-failing participants), 22 (governing the establishment of "Bilateral Limits" by each participant for each other participant).

<sup>918</sup> *Id.* Rule 13(h).

<sup>919</sup> See *id.* Rule 13(h).

<sup>920</sup> See *id.* Rule 23.

<sup>921</sup> Memorandum from John F. Lee, Executive Vice President, NYCHA, to the NYCHA Clearing House Committee, Attachment A ("Loss Sharing Formula") (Apr. 28, 1989) ("There is a possibility, however remote, that the application of the formula for multiple bank failures will produce amounts that exceed the limitations. Should that occur a participant or group of participants may voluntarily agree to contribute the excess for themselves or for others. . . .").

<sup>922</sup> CHIPS Rule 13(k).



foregoing loss allocation scheme is for each participant in effect to establish its own maximum level of liability by manipulating the bilateral limits it grants to other participants. The extent of liability is an indirect function of the member's usage of CHIPS, and discipline is enforced by means of the collateralization requirement.

Another means of allocating risk, by number of messages sent, governs different risks and losses. CHIPS has entered into a "Settlement Agreement" with the Federal Reserve Bank of New York (the "FRBNY") pursuant to which the FRBNY receives funds from certain participants with debit positions and delivers the proceeds to participants with credit positions on a daily basis. Amounts, if any, remaining in the settlement account at FRBNY after 6:00 p.m. may be transferred by FRBNY to the Fed account of the so-called "Six O'Clock Bank," as custodian.<sup>923</sup> All CHIPS participants are responsible for indemnifying both the FRBNY for "claims" and the Six O'Clock Bank for "loss, liability or expenses . . . arising from its acts or omissions . . . except for [those] arising from . . . willful failure . . . ." <sup>924</sup> Rule 14(e) requires participants to share indemnification obligations ratably on the basis of their proportional "Average Daily CHIPS Usage,"<sup>925</sup> which is defined as the average daily number of payment messages released and received over the prior thirty days.<sup>926</sup>

The CHIPS Rules also disclaim liability "to any participant or any other person for any loss, liability or expense . . . arising from the Clearing House's acts or omissions in connection with the system."<sup>927</sup> In the event NYCHA is found liable, however, all participants, again, have agreed to indemnify it ratably according to their Average Daily CHIPS Usages.<sup>928</sup>

The "quantity-based" risk allocation scheme of the CHIPS Rules appears to reflect Article 4A's rejection of consequential damages.<sup>929</sup> Because any claim against the FRBNY, the Six O'Clock Bank, or NYCHA itself will likely not include

---

<sup>923</sup> See generally *id.* Rule 14; *id.* Rule 13(c).

<sup>924</sup> *Id.* Rule 14(a), (c).

<sup>925</sup> *Id.* Rule 14(e).

<sup>926</sup> See *id.*

<sup>927</sup> *Id.* Rule 15.

<sup>928</sup> See *id.*

<sup>929</sup> See U.C.C. § 4A-305(c).

consequential damages, there is little rationale for varying participants' indemnification liability by their dollar-volume importance to the system. This quantity-based risk allocation scheme is appropriate when damages would be limited to costs of re-transmitting messages or the like, which costs do not vary substantially by the dollar amount of the message, but seems less appropriate were the FRBNY or the "Six O'Clock Bank" to "lose" a day's worth of debit or credit positions.

CHIPS Rule 16 might appear to suffer from the same deficiency, but in fact it does not. Rule 16(a) provides, sensibly, that participants are responsible for "fraudulent transfers" originating at their respective banks. However, participants again share liability according to their thirty-day average daily number of payment messages released and received for fraudulent transfers initiated at the NYCHA, once the mandated \$25 million of insurance has been exhausted.<sup>930</sup> Apparently, the notion is that a NYCHA-initiated fraudulent transfer is a risk unrelated to the dollar volume used by each participant and should be allocated on a formula similar to that used for other operating expenses.<sup>931</sup>

## 5. Fedwire

"Fedwire" is the funds-transfer system owned and operated by the Federal Reserve Banks.<sup>932</sup> "Regulation J" of the regulations promulgated under the Federal Reserve Act governs "Funds Transfers Through Fedwire."<sup>933</sup> The liability of a Federal Reserve Bank (an "FRB") with respect to Fedwire transfers is limited and, in certain respects, even more restricted than comparable undertakings by the commercial banking system.<sup>934</sup> The following provides relevant examples of liability limitations in the Fedwire context:

---

<sup>930</sup> CHIPS Rule 16(b).

<sup>931</sup> See *id.* Rule 11.

<sup>932</sup> See 12 C.F.R. § 210.26(e).

<sup>933</sup> *Id.* §§ 210.25 *et seq.* Subpart B was promulgated pursuant to 12 U.S.C. §§ 342, 464(f), 248(i), (j), (o), "and other laws." 12 C.F.R. § 210.26(a). Pursuant to 12 C.F.R. § 210.25(c), "[e]ach Federal Reserve Bank shall issue an Operating Circular consistent with this subpart that governs the details of its funds-transfer operations and other matters it deems appropriate. . . . [including] available security procedures . . . and . . . charges for funds-transfer services." *Id.* § 210.25(c).

<sup>934</sup> See Operating Circular on Reserve Bank Liability §§ 49-54.



- Consequential Damages. An FRB "shall not be liable to a sender, receiving bank, beneficiary, or other Federal Reserve Bank, governed by this subpart, for any damages other than those payable under Article 4A. A Federal Reserve Bank shall not agree to be liable to a sender, receiving bank, beneficiary, or other Federal Reserve Bank for consequential damages under section 4A-305(d) of Article 4A."<sup>935</sup>
- Identification of Payees. An FRB may rely on account numbers alone and has no duty to detect an inconsistency in identification between the name in the payment order and the number identifying the intermediary, beneficiary's bank, or the beneficiary.<sup>936</sup>
- Notice: Thirty days is specified as a reasonable time within which the sender of a payment order to a FRB must notify the FRB "of the relevant facts concerning an unauthorized or erroneously executed payment order . . . after the sender receives notice that it was accepted or executed" for purposes of sections 4A-204(a) and 4A-304 of Article 4A.<sup>937</sup>
- Discretion: "A Federal Reserve Bank may reject, or impose conditions that must be satisfied before it will accept, a payment order for any reason."<sup>938</sup>
- Security: "A Federal Reserve Bank may require a sender to execute a written agreement concerning security procedures or other matters before the sender may send payment orders to the Federal Reserve Bank."<sup>939</sup>

Also, the Fedwire rules and Article 4A address the applicability of a funds-transfer system as well as choice of law. Such rules might provide a useful starting point

---

<sup>935</sup> 12 C.F.R. § 210.32(a).

<sup>936</sup> *See id.* § 210.27(a), (b). This is a slightly different rule than that which pertains under Article 4A generally. *See* U.C.C. § 4A-208(b).

<sup>937</sup> 12 C.F.R. § 210.28(c); *see* U.C.C. § 4A-208(b)(2) ("Proof of notice may be made by any admissible evidence. The receiving bank satisfies the burden of proof if it proves that the sender, before the payment order was accepted, signed a writing stating the information to which the notice relates.").

<sup>938</sup> 12 C.F.R. § 210.30(a).

<sup>939</sup> Appendix A ("Commentary") to "Regulation J, Subpart B" (12 C.F.R. §§ 210.25 *et seq.*) at *id.* § 275 (1993).

in analyzing the applicability of, and the relation among, rules of various certification authorities in the absence of privity.<sup>940</sup>

## 6. S.W.I.F.T.

In 1973, an international group of bankers founded the Society for Worldwide Interbank Financial Telecommunications ("S.W.I.F.T.").<sup>941</sup> Although S.W.I.F.T. is used to communicate a variety of standardized, legally operative financial communications,<sup>942</sup> it is only a communications network and does not perform settlement functions.<sup>943</sup> S.W.I.F.T. directs messages over facilities leased from national postal telephone and telegraph authorities.<sup>944</sup>

With respect to the allocation of risk for error or fraud, one commentator has analogized the liability of parties to "joint venturers in a carriage-of-messages enterprise."<sup>945</sup> Fundamentally, S.W.I.F.T. has disclaimed liability "for any segment of the transmission not directly under its control."<sup>946</sup> Thus, S.W.I.F.T. is not responsible for technical failure, force majeure, or the transmission of unauthorized messages, unless it could have reasonably assessed the validity thereof.<sup>947</sup> Conversely, S.W.I.F.T. has accepted liability for the negligence, failure

---

<sup>940</sup> See U.C.C. §§ 4A-501(b), 4A-507(c), 12 C.F.R. § 210.25(b) and corresponding commentary in Appendix A thereof.

<sup>941</sup> Byler & Baker, *S.W.I.F.T.: A Fast Method to Facilitate International Financial Transactions*, 17 J. WORLD TRADE L. 458, 460 (1983).

<sup>942</sup> Two sorts of communications are CHIPS messages, *see id.* at 462, and "paperless" letters of credit. *See* Kozolchyk, *The Paperless Letter of Credit with Related Documents of Title*, 55 L. & CONTEMP. PROBS. 39 (summer 1992). *See generally* UNCITRAL, Working Group on International Contract Practices of the 20th sess. concerning Independent Guarantees and Stand-by Letters of Credit (A/CN.9/WG.II/WP.80) (Oct. 12, 1993).

<sup>943</sup> *See* Byler & Baker, *supra* note 941, at 458.

<sup>944</sup> *See id.*

<sup>945</sup> Kozolchyk, *supra* note 942, at 58.

<sup>946</sup> *Id.* at 55 (citing S.W.I.F.T. User Handbook version 1.0, 89/4 [hereinafter S.W.I.F.T. Rule(s)] 21.5.1., 22.1.2.1).

<sup>947</sup> *See id.* at 56 (citing S.W.I.F.T. Rule 23.1).



to use security procedures and fraud of its own personnel.<sup>948</sup> S.W.I.F.T. is not liable for consequential damages,<sup>949</sup> and its "per occurrence" and annual liability for non-interest losses is subject both to caps<sup>950</sup> and to a "deductible" of two million Belgian francs.<sup>951</sup> Excess liability is apportioned among members according to their annual "amount of messages."<sup>952</sup> Ten years ago, S.W.I.F.T. was reported as carrying liability insurance.<sup>953</sup>

The S.W.I.F.T. Rules also allocate liability for lost interest arising from delay among senders, receivers and S.W.I.F.T. itself. Thus, S.W.I.F.T. is liable for delay when it fails to deliver a message and to report such failure on an "Undelivered Message Report" ("UMR") to the sender, as well as for failing to report technical difficulties in a timely fashion.<sup>954</sup>

Senders are liable, *inter alia*, for failing to "catch" a UMR or absence of acknowledgment of receipt by the S.W.I.F.T. system; for utilizing an inappropriate messaging format or faulty information; and for ignoring messages from

---

<sup>948</sup> See *id.* (citing S.W.I.F.T. Rule 23.4.2 ) (negligence and failure to use security procedures).

<sup>949</sup> See *id.* at 57 (citing S.W.I.F.T. Rule 23.4.2).

<sup>950</sup> S.W.I.F.T.'s maximum liability on an "occurrence" basis is three billion Belgian francs. The annual cap is six billion Belgian francs. See *id.* (citing S.W.I.F.T. Rule 23.4.3).

<sup>951</sup> *Id.* (citing S.W.I.F.T. Rule 23.5.2).

<sup>952</sup> *Id.* Prof. Kozolchyk's unhappily worded formulation probably refers to the financial size of messages, rather than to their number. A "fair" measurement of this figure presents problems. The "amount," for example, of a payment order is easily determined. But the face amount of a standby letter of credit might, on some theories, require a deduction to account for the possibility that the beneficiary will not draw upon it. Again, in the event the beneficiary draws upon a letter of credit, the issuer may or may not be "charged" a second time for the actual payment message.

<sup>953</sup> Byler & Baker, *supra* note 941, at 458.

<sup>954</sup> Kozolchyk, *supra* note 942, at 57 n.77 (citing S.W.I.F.T. Rule 22.4.3). Again, S.W.I.F.T.'s liability is capped (at fifty million Belgian francs) and subject to a "deductible" (100,000 Belgian francs). Excess losses are allocated among members. See *id.* at 57-58 (citing S.W.I.F.T. Rule 23.5.2).

S.W.I.F.T. regarding difficulties.<sup>955</sup> Receivers bear the loss when they fail to reconcile their receipt of messages by sequence number and to respond to notices from S.W.I.F.T. and to other manifest indicia of possible problems.<sup>956</sup>

Although certain commentators have criticized the S.W.I.F.T. rules for failing to observe the "cheapest cost avoider" principle in every respect<sup>957</sup> and to provide for compensation for exchange losses precipitated by delay,<sup>958</sup> Professor Kozolchyk has made the (perhaps facile) conclusion that, "judging from the mushrooming number of S.W.I.F.T. users and from the continuing low cost of the service, [S.W.I.F.T.] has worked well."<sup>959</sup>

## 7. Special Risk Allocation Schemes - Consumer Transactions

Certain features of federal "consumer protection" legislation in the area of payment systems law also merit consideration, including those contained in the Electronic Fund Transfer Act of 1978 ("EFTA")<sup>960</sup> and the provisions of the Truth-in-Lending Act<sup>961</sup> dealing with credit cards. Although this Report assumes that consumers will not for the time being be encouraged, required, or permitted to avail themselves of FCA services, this legislation is relevant, for several reasons. First, the FCA may issue certificates, or FCA-users may hold their private keys and/or create digital signatures, using a card technology in a form analogous to

---

<sup>955</sup> See *id.* at 57-58 n. 77 (citing S.W.I.F.T. Rule 22.4.4).

<sup>956</sup> See *id.* at 58 n.77 (citing S.W.I.F.T. Rule 22.4.5).

<sup>957</sup> See Lingl, Comment, *Risk Allocation in International Interbank Electronic Fund Transfers: CHIPS and S.W.I.F.T.*, 22 HARV. INT'L L.J. 621 (1981).

<sup>958</sup> Ambrosia, Note, *New S.W.I.F.T. Rules on the Liability of Financial Institutions for Interest Losses Caused by Delay in International Fund Transfers*, 123 CORNELL INT'L L.J. 311, 325-27 (1980) (explicated in Kozolchyk, *supra* note 942, at 59 n.85).

<sup>959</sup> Kozolchyk, *supra* note 942, at 58. S.W.I.F.T.'s "mushrooming numbers" and the compliance of its members, however, are more likely to be the result of an absence of significant losses and the lack of suitable alternatives than of a general *ex ante* approbation of its liability scheme.

<sup>960</sup> 15 U.S.C. §§ 1693 *et seq.*

<sup>961</sup> *Id.* §§ 1601 *et seq.* "Regulation E" contains regulations of the Federal Reserve Board's regulations implementing the EFTA. See 12 C.F.R. § 205.1(a).



traditional credit, debit, or automated teller machine ("ATM") cards. Second, consumer protection legislation in the payment systems area can be viewed as a means for consumers to deal with organizations, systems and processes that are somehow "beyond" them. To the extent that establishment of the FCA would constitute a radical departure from existing practices, similar protections may be appropriate even for sophisticated business concerns. Finally, the federal government itself has arguably entered this area as a major participant in the operational aspects of payment systems law by virtue of amendments to *Regulation E* to cover governmental benefit transfers.

#### a. The Electronic Fund Transfer Act

EFTA deals with "electronic fund transfer" to or from the "account" of a "consumer."<sup>962</sup> *Electronic funds transfer* is defined to mean "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account."<sup>963</sup> A *consumer* is a natural person,<sup>964</sup> and an *account* is a "demand deposit, savings deposit, or other asset account . . . established primarily for personal, family or household purposes . . ."<sup>965</sup>

EFTA and Regulation E impose certain requirements of disclosure and documentation, allocate risk for various mishaps and establish a dispute resolution scheme. In terms of disclosure and documentation, EFTA mandates that the consumer be apprised of his legal rights and remedies in respect of electronic funds transfer and the applicable charges therefor.<sup>966</sup> Consumers have

---

<sup>962</sup> 15 U.S.C. §§ 1693, 1693a.

<sup>963</sup> *Id.* § 1693(6). This section goes on to provide an illustrative list of electronic fund transfers, which includes point of sale ("POS") transfers; ATM transactions; direct deposits or withdrawals of funds, and transfers initiated by telephone. *See id.* A series of exempt transactions is also enumerated. *See id.*; cf. 12 C.F.R. §§ 205.1 *et seq.*; Board of Governors of the Fed. Reserve Sys., Official Staff Commentary on Reg. E (Electronic Fund Transfers) [hereinafter REG. E STAFF COMMENTARY].

<sup>964</sup> *See* 15 U.S.C. § 1693(5).

<sup>965</sup> *Id.* § 1693(2).

<sup>966</sup> *See id.* § 1693c.

the right to receive documentation of each transfer and periodic statements of account activity as well.<sup>967</sup>

EFTA's risk allocation scheme is interesting from the standpoint of the FCA. Financial institutions are liable "for all damages proximately caused" by the failure to make a transfer in accordance with the terms and conditions of an account, by wrongful dishonor of a transfer and by failure to observe a stop-payment order.<sup>968</sup> However if the breach was not intentional, and resulted from bona fide error "notwithstanding the maintenance of procedures reasonably adapted to avoid any such error," then damages are limited to actual damages proved.<sup>969</sup> Finally, the financial institution is absolved from *all* liability if its breach resulted from an "act of God or other circumstances beyond its control" or from "a technical malfunction known to the consumer"<sup>970</sup> in the case of failing to make an appropriate transfer or upon wrongful dishonor.

Section 1693g governs the liability of consumers for unauthorized transfers. In general, no consumer can be liable for a transfer unless he has "accepted" a "card or other means of access" which permits third parties to identify the person authorized.<sup>971</sup> Further, a consumer's liability for an unauthorized transfer is capped at the lesser of \$50 or the aggregate amount of unauthorized transfers occurring prior to the time the consumer gives notice to the financial institution, unless the consumer (i) gives untimely notice of loss or theft, in which case liability is capped at the lesser of \$500 or the losses which could have been prevented by the giving of timely notice, or (ii) fails to report unauthorized transfers appearing on a periodic statement in a timely manner, in which case there is no cap on liability.<sup>972</sup> Apart from these notification requirements, EFTA imposes *no* duty of care on consumers with respect to the safe-guarding of access devices.<sup>973</sup> Moreover, the financial institution bears the burden of proof on the

---

<sup>967</sup> See *id.* § 1693d.

<sup>968</sup> *Id.* § 1693h(a).

<sup>969</sup> *Id.* § 1693h(c).

<sup>970</sup> *Id.* § 1693h(b).

<sup>971</sup> *Id.* § 1693g(a).

<sup>972</sup> See *id.*; see also 12 C.F.R. § 205.6(b).

<sup>973</sup> Thus, a consumer who writes his access code on an ATM card or on a piece of paper kept with the card would *not* impair his rights under EFTA. See REG. E STAFF COMMENTARY, *supra* note 963, at Q6-6.5 ("The extent of the consumer's liability is determined by the promptness in reporting loss or theft of an access



issue of authorization and, if necessary, on the issue of the consumer's liability under the foregoing.<sup>974</sup> Obviously, this burden will often prove insuperable.

It is not recommended that user-key holders be absolved from responsibility to this degree. They, rather than the FCA, are able to assess the potential for financial or other consequences of key compromise. Moreover, the absence of any analog to account depletion in the FCA area means that no "automatic" cap on liability exists. Finally, EFTA's limitation on consumer liability, if applied in the FCA area, might be considered inimical to user responsibilities legitimately associated with "high assurance" implementations and corresponding presumptions otherwise intended to be established for reliance on certificates within the purview of the FCA.

EFTA's dispute resolution scheme requires financial institutions to investigate and respond to notice of alleged errors within certain time limits.<sup>975</sup> Damages may be trebled for investigations not conducted in good faith.<sup>976</sup> Because FCA-related disputes and claims are likely to be more complex, less stereotypical and involve greater amounts of value than those arising under EFTA, this approach may not be practicable in the FCA context.

Last, EFTA provides a scheme of civil and criminal liability for violations of its provisions. The most salient provisions of civil liability are that consumers are entitled to a "penalty" (between \$100 and \$1,000, presumably so as not to discourage cases of minimal financial import from being brought) and that damages are capped in class actions to the lesser of \$500,000 or 1% of the

---

device or unauthorized transfer appearing on a periodic statement. Negligence on the consumer's part cannot be taken into account to impose greater liability than is permissible under the act and Regulation E.").

EFTA's paternalist nature is amply illustrated by comparing it to the "damn fool" doctrine in the law of insurance, which precludes the transfer risk (insurance coverage) for "incredibly foolish conduct." KEETON & WIDISS, *supra* note 16, § 5.4(E), at 539-41.

<sup>974</sup> See 15 U.S.C. § 1693g(b).

<sup>975</sup> See *id.* § 1693f(a)-(d). See generally Section IX.D.4., *infra* (concerning alternative dispute resolution mechanisms).

<sup>976</sup> See 15 U.S.C. § 1693f(e).

defendant's net worth.<sup>977</sup> EFTA's criminal provisions appear in section 1693n and are broadly drafted.<sup>978</sup>

In the short term, EFTA's direct applicability to FCA-related applications would appear to be minimal, given the limited role consumers are expected to play in early experimental implementations.<sup>979</sup> Nonetheless, EFTA confers broad authority on the Federal Reserve Board of Governors by regulation to "provide for such adjustments and exceptions from any class of fund transfers . . . to effectuate the purposes of this subchapter, to prevent circumvention or evasion thereof, or to facilitate compliance therewith."<sup>980</sup> The Board's authority is a function of whether the transfers are initiated electronically, whether current laws provide adequate consumer safeguards, and whether coverage is necessary to achieve the Act's basic objectives. Congress contemplated that, as no person can foresee EFT developments, "regulations would keep pace with new services and assure that the act's basic protections continue to apply."<sup>981</sup>

These issues have come to the fore in recent months as a result of proposals to amend Regulation E, including to cover electronic benefit transfer ("EBT") initiatives.<sup>982</sup> Concern was raised, for example, by the State of Michigan, which objected to the proposed amendments on the basis, *inter alia*, that making EBT subject to Regulation E might have the unexpected impact of causing teller-operated food stamp dispensing systems to become subject to Regulation E and that a state should not bear the same liability as a "financial institution" in the event a benefit recipient loses his card or compromises his access device:

In private industry, if a loss is not the liability of the consumer, it is absorbed by the financial institution. With EBT programs, the loss will be absorbed by the government

---

<sup>977</sup> *Id.* § 1693m(a).

<sup>978</sup> *See id.* § 1693n.

<sup>979</sup> *See* Section IV.H., *supra* (stating the assumption that the FCA will not, at least not initially, support consumer transactions).

<sup>980</sup> 15 U.S.C. § 1693b(c). "This provision is virtually identical to section 105 of the Truth-in-Lending Act, a provision interpreted by the United States Supreme Court as granting the Board great discretion in defining coverage. The Court consistently has recognized Congress' delegation of broad authority to the Board." 58 Fed. Reg. 8714 (Feb. 17, 1993).

<sup>981</sup> S. Rep. No. 95-915, 95th Cong., 2d sess. (Sept. 10, 1978).

<sup>982</sup> *See* 59 Fed. Reg. 10,684 (Mar. 7, 1994); 58 Fed. Reg. 8,714 (Feb. 17, 1993) (setting forth Proposed Regulation 12 C.F.R. § 205.15).



agency, which is deemed to be a financial institution under the proposed regulation. Unlike financial institutions, governments cannot limit their liability for such losses by pre-screening the credit history of recipients or recouping losses by charging interest to cardholders.<sup>983</sup>

The final EBT rule amends the definition of "account" to include "an account established by a government agency for distributing government benefits to a customer electronically, such as through ATMs or POS terminals, whether or not the account is directly held by the agency or a bank or other depository institution." It also notes that "periodic statements are not absolutely necessary for EBT programs [because they] could impede the efforts to eliminate paper and move toward a fully electronic system."<sup>984</sup>

## **b. Truth-in-Lending Act and Credit Cards**

The provisions in the Truth-in-Lending Act that deal with credit cards address many of the same concerns, and in the same fashion, as EFTA. Indeed, the Truth-in-Lending Act and related legislation provided an important precedent for EFTA's "concepts and techniques for legal control."<sup>985</sup> Thus the Consumer Credit

---

<sup>983</sup> Letter from Gerald Miller, State of Michigan to William Wiles, Secretary, Board of Governors of the Fed. Reserve Sys. (Apr. 14, 1993) (copy on file at Independent Monitoring). The letter also raised the issue as to whether "smart cards" are covered by Reg. E. Consider the following:

If the FCA is implemented using card technologies, [portions of] such card usage would probably be interpreted as coming under the purview of Reg. E. However, historically, the federal government has tended to exempt itself from Regulation E, and instead implemented alternative regulations. The exclusion of FCA users from Reg. E is critical to ensure card holder accountability for their negligent and fraudulent acts.

Interview with George Usher, Financial Management Servs., U.S. Treasury Dep't (July 27, 1993).

"[L]iability is being viewed by many states as an insurmountable challenge." T. Fashingbauer, *Will Banking Regulation Kill EBT?*, GOVERNMENT TECHNOLOGY, May 1994 at 32.

<sup>984</sup> 59 Fed. Reg. 10,678 (Mar. 7, 1994) (to be codified at 12 C.F.R. § 205 *et seq.*).

<sup>985</sup> Brandell & Olliff, *The Electronic Fund Transfer Act: A Primer*, 40 OHIO ST. L.J. 531, 537 (1979). The Truth-in-Lending Act can be found at 15 U.S.C. § 1601 *et seq.*, as implemented by Regulation Z, 12 C.F.R. § 226.

Protection Act provides for comprehensive disclosure and account activity reporting requirements,<sup>986</sup> a billing resolution scheme similar to that of EFTA,<sup>987</sup> and limitations on card holder liability for unauthorized use.<sup>988</sup> Minimum and maximum levels of civil liability are substantially identical to those under EFTA,<sup>989</sup> and a "safe harbor" for unintentional violations resulting from a "bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error" is provided.<sup>990</sup> Criminal penalties are sprinkled liberally throughout.<sup>991</sup>

The Truth-in-Lending Act goes beyond EFTA in several important respects, however. First, businesses which provide employees with credit cards, pursuant to the Truth-in-Lending Act's exemption for "[c]redit transactions involving extensions of credit primarily for business . . . purposes,"<sup>992</sup> may contract with card issuers respecting liability for unauthorized use.<sup>993</sup> However, "in no case may such business or other organization or card issuer impose liability upon any employee with respect to unauthorized use of such a credit card except in accordance with and subject to the [U.S. \$50 and other] limitations of section [1643]."<sup>994</sup> Moreover, the Truth-in-Lending Act endows consumers with specific

---

<sup>986</sup> See 15 U.S.C. §§ 1631-1634, 1637-1638; Section V.B.4.e., *supra* (concerning auditing and accounting).

<sup>987</sup> See 15 U.S.C. §§ 1666-1666h.

<sup>988</sup> See *id.* § 1643. Unlike EFTA's multi-tiered structure, however, the Truth-in-Lending Act sets a maximum liability of \$50. See *id.* § 1643(a)(1)(B). Like EFTA, however, the card holder's negligence is irrelevant to his liability, and the card issuer bears the burden of proof on authorization. See *id.* § 1643(b).

<sup>989</sup> See *id.* 15 U.S.C. § 1640(a)(2).

<sup>990</sup> *Id.* § 1640(c). "Examples of a bona fide error include, but are not limited to, clerical calculations, computer malfunction and programming, and printing errors." *Id.*

<sup>991</sup> See, e.g., *id.* §§ 1611, 1644.

<sup>992</sup> *Id.* § 1603(1). But see *id.*, § 1645 (concerning business credit cards).

<sup>993</sup> See *id.* § 1645. Cf. Section IX.D.2., *infra* (concerning the permissibility of contracting for commercially unreasonable security procedures pursuant to the UNCITRAL draft EDI Statutory Provisions).

<sup>994</sup> 15 U.S.C. § 1645.



rescission rights for certain especially sensitive transactions,<sup>995</sup> and renders certain defenses of the card holder against a merchant effective against the card issuer.<sup>996</sup>

The following table illustrates differences in credit card and certificate issuance procedures that may have an impact on approaches to FCA infrastructure.

	CREDIT CARD	PUBLIC KEY CERTIFICATE Implementing a <i>low-medium</i> assurance policy
Personal Presence for Issuance	no	most likely
Investigation for Issuance	yes (e.g., Equifax and TRW )	little or none beyond ID documents
"Preapproval"	some	none
Authorization	credit limit and/or card class	attribute cert., implied, other
Revocation	restricted card list or on-line	CRL
Used to Establish Identity	sometimes on a <i>de facto</i> basis	yes (cf. persona certificates)

TABLE 2 - CREDIT CARD & CERTIFICATE ATTRIBUTES COMPARED

## B. VALUE ADDED NETWORKS

Value Added Networks ("VANs")<sup>997</sup> present liability issues that provide important insight in analyzing and developing an FCA liability scheme. These liability issues assist the FCA developer because:

- VANs provide diverse information services, many of which require security protections.
- VANs will continue to dominate the non-classified private and public sectors.
- VANs are likely to offer certificate and key management services increasingly.

<sup>995</sup> See, e.g., *id.* § 1635 (applicable to "any consumer credit transaction . . . in which a security interest . . . is or will be retained or acquired in any property which is used as the principal dwelling of the person to whom credit is established").

<sup>996</sup> See *id.* § 1666i.

<sup>997</sup> VANs can be defined as a subset of Third Party Service Providers ("TPSPs"). TPSPs provide, at a minimum, communications transport service. VANs provide *value added* services: not simply a communications channel, but rather the provision of, e.g., information, data processing, directory, or format translation services. See generally ELECTRONIC CONTRACTING, *supra* note 2, ch. 3.

- d. VANs have significant experience in managing liability under schemes established by agreement and tariff; many have also considered insurance and technical means of managing risk.
- e. VANs have been the focal point for much of the debate related to third-party liability.
- f. VANs and the FCA will necessarily interact, and will need to be mutually accommodating on a variety of fronts.

VANs and the FCA will also perform distinct functions:

- a. VANs may freely contract to provide communication services only.
- b. VANs and their users may implement FCA services to transfer administrative duties and responsibility for a portion of security services.
- c. VANs cannot control communications on an end-to-end basis, particularly when multiple VANs are interconnected; FCA services are intended to provide assurance for end-to-end communications.
- d. The FCA will be able to service users of many VANs.

Given these differences, the ultimate question is whether and how FCA liability should be distinguished from that of VANs.<sup>998</sup>

The following commentary on the scope of appropriate VAN liability largely reflects the position of VANs generally:

[A service provider] will attempt to limit its responsibilities to a level which is commensurate to the fees charged for the service. . . . In terms of warranties the users clearly have a right to expect that the EDI service will do what the service provider says it will do. . . . The service provider's obligations with respect to performance warranties should be limited to what the service provider represents about the service, not what the user may expect from it. . . . In light of the nominal amount of EDI service charges and the fact that the service provider receives no benefits whatsoever from the underlying transaction, it seems highly inappropriate to assert that they should be exposed to any liability in excess of the typical limitation [*e.g.*, fees paid for a certain period and disclaimer of consequential damages]. Furthermore, since the trading partners are the parties who know the nature and terms of the underlying transactions they are clearly in the best position to implement appropriate checks and controls to minimize any potential risks resulting from an EDI service failure. Therefore, the typical limitations of liability provision represents a reasonable allocation of those risks.<sup>999</sup>

---

<sup>998</sup> See *Shell Pipeline v. Coastal States Trading*, 788 S.W.2d 837 (Tex. App. 1990) (holding that negligent provision of even gratuitous services was actionable); *supra* note 142.

<sup>999</sup> B. Hunter, *Legal Responsibilities of EDI Service Providers: A Service Provider's Perspective*, in PROCEEDINGS OF EDI AND THE LAW '91 (Data Interchange Standards Association 1991). This is strikingly consistent with the



## Caps on VAN Liability

Consistent with this position, most VAN agreements contain extensive disclaimers and limitations on liability. Perhaps most revealing, however, are the caps on liability that most agreements provide. These caps limit the total amount of recoverable damages to a specific amount or formula or disclaimer and liability limitation clauses. These caps may also reflect a VAN's determination of the minimum level of liability it must be prepared to absorb in order to ensure enforceability of its agreements. In most cases, VANs provide for a general disclaimer of all but direct damages, and frequently limit exposure to the lesser of actual damages or fees paid under the VAN agreement, or to some liquidated sum.

The following table compares caps on liability for several service providers:

---

rationale for precluding consequential damages under Art. 4A. See R. GOTTLIEB, *supra* note 879. Cf. Wang, *The Liability of Electronic Data Interchange Network Operators* (TEDIS, July 1991).

SERVICE PROVIDER (EDI VAN)	CAP ON LIABILITY
AT&T	An amount not to exceed \$100,000 <sup>1000</sup>
BT America	Previous 12 months usage charges <sup>1001</sup>
G.E. Information Services	Greater of 3 mo. average cost over past 12 mos., or \$10,000
Ordernet Services	Previous 30 days payments <sup>1002</sup>

1000

B. AT&T'S ENTIRE LIABILITY . . . SHALL BE: (1) FOR IMPROPER PERFORMANCE OR NON-PERFORMANCE OF MESSAGING SERVICE(S), INCLUDING SUPPORT FACILITIES, THE REMEDY SET FORTH IN PARAGRAPH . . . [PERFORMANCE WARRANTY] (2) FOR FAILURE OF SOFTWARE LICENSED BY AT&T, THE REMEDY SET FORTH IN PARAGRAPH . . . OR IN THE AGREEMENT ACCOMPANYING THE SOFTWARE, IF APPLICABLE, (3) FOR DAMAGES TO REAL OR TANGIBLE PERSONAL PROPERTY OR FOR BODILY INJURY OR DAMAGES TO PROPERTY OR PERSON, (4) FOR CLAIMS OTHER THAN SET FORTH ABOVE, AT&T'S LIABILITY SHALL BE LIMITED TO DIRECT DAMAGES WHICH ARE PROVEN, IN AN AMOUNT NOT TO EXCEED \$100,000.

AT&T VAN Agreement § 11A-11D (emphasis added).

1001 "[Service Provider]'s entire liability to [Customer] for damages of any cause whatsoever, and regardless of the form of action, shall be limited to the lesser of [i] [Customer]'s actual direct damages or [ii] the amount paid to the [Service Provider] under this [VAN agreement] for the immediately preceding twelve [12] months." BT America VAN Agreement § X.H.

"In the event that such remedies are not economically feasible, [Service Provider] will accept [Customer]'s termination of this [VAN agreement] and [Service Provider] agrees to refund to the [Customer] the previous six (6) months usage charges incurred under this [VAN agreement]." *Id.* § X.Q.

1002 Ordernet Services Agreement § 7(d) ("In no event shall the aggregate [liability] exceed payments made with respect to the thirty days of service immediately preceding date of breach by the Service Provider.").

1002A This proposed limitation of liability appears in a report developed by a multi-agency federal task force assembled under the co-leadership of GSA and DoD.

The provider is not expected to assume liability for incidental, special, or consequential damages or for third-party claims made by non-EDI VAN clients against the provider or the government, under or related to the agreement. The provider's total liability . . . will not exceed, in the aggregate, \$100,000.



Harbinger*EDI Services., Inc.	None
U.S. Gov't (proposed for VANs)	Not to exceed 100,000 <sup>1002A</sup>

**TABLE 3 - COMPARISON OF VAN LIABILITY CAPS**

Most of the foregoing liability caps were not developed, and cannot be supported, scientifically.<sup>1003</sup> Rather, as described by counsel to one of the above TPSPs, liability caps are nothing more than a "gut assessment" and had been in use since the time when the TPSP was in the time-sharing business. Counsel representing the other TPSPs that were contacted could, at best, advance policies in support of caps generally, but could not otherwise present a cogent argument in support of particular amounts. The situation may well be a reasonable response to the experience and belief that TPSPs do not face strict liability for engaging in inherently dangerous activities.<sup>1004</sup>

---

Federal Electronic Commerce Acquisition Team, Streamlining Procurement Through Electronic Commerce, app. G (Final Draft, Apr. 29, 1994).

<sup>1003</sup> However, counsel to one international TPSP stated, under condition of anonymity, that: "In order for EDI to be provided in a competitive, non-regulated environment in a low cost structure, providers must be free to assess the risk they can economically bear. A higher liability exposure necessitates a higher fee for the service. Regulated service has its liability set by the regulating organization, which in most cases will not require liability for all actions. Hence, in effect, there is a cap there, as well. If a user wants to pay more, a VAN can offer greater assurance from error." Letter to M. Baum (Sept. 20, 1993).

<sup>1004</sup> Some TPSPs assert that they do not face exposure based on strict liability because of the absence of the likelihood of personal injury. Cf. Section VI., *supra* (considering, in part, whether a requirement of personal injury for certain kinds of actions and damages is eroding).

## VAN Interconnection Agreements

In order to facilitate communications between trading partners that are connected to different third party service providers, many VANs interconnect their systems or networks. The rights and responsibilities associated with the communications link between VANs are typically expressed in an "interconnect" or "interconnection" agreement, which is executed between VANS to facilitate end-user interconnection. Consideration should also be given to the apportionment of liability established within the context of interconnection agreements between and among VANs. The following interconnect agreement clauses are intended to limit liability.

[Service Provider 1] AND [Service Provider 2] HEREBY DISCLAIM ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.<sup>1005</sup>

IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY, THE SUBSCRIBERS OF THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY LOST OR DISTORTED IMAGES, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES AS A RESULT OF PERFORMANCE OR NON-PERFORMANCE OF THE SERVICES PROVIDED PURSUANT TO THIS AGREEMENT, INCLUDING WITHOUT LIMITATION DAMAGES TO OR DESTRUCTION OF DATA, INFORMATION FILES OR DATABASES, LOSS OF PROFITS OR OTHER ECONOMIC LOSS.<sup>1006</sup>

EACH PARTY WILL INDEMNIFY AND HOLD HARMLESS THE OTHER PARTY FOR ANY AND ALL CLAIMS (INCLUDING WITHOUT LIMITATION COSTS, EXPENSES, AND REASONABLE ATTORNEY'S FEES) MADE BY THE INDEMNIFYING PARTY'S SUBSCRIBERS WHICH ARISE OUT OF THE SERVICES PROVIDED PURSUANT TO THIS AGREEMENT.<sup>1007</sup>

The extent to which such approaches are properly transferable to FCA arrangements, or among cross-certifying entities, requires determination.

## The Relevance of Value-Added Network Agreements

It is evident that VAN agreements provide a useful starting point in considering the scope and content of FCA agreements. VANs share important attributes with the FCA in that they (i) act as intermediaries in support of telecommunications;

---

<sup>1005</sup> AT&T Interconnection Agreement § 5.1.

<sup>1006</sup> *Id.* § 5.2.

<sup>1007</sup> *Id.* § 5.3.



(ii) provide a degree of information security; (iii) typically have more bargaining power than their users; (iv) may often offer CA services in the future; and (v) seek to minimize or rigorously control their liability (and have apparently been largely successful in doing so thus far), particularly with respect to consequential damages.<sup>1008</sup> Consequently, trends in VAN exposure, as indicated by case law, agreements and by industry practices, as well by the introduction of enhanced security services by VANs, and the terms and conditions under which such services are provided, deserve close monitoring by the FCA.<sup>1009</sup>

---

<sup>1008</sup> One longer-term problem with disclaimers such as those VANs employ is that they are resource-intensive: each party must execute an agreement and parties will invariably seek to negotiate its terms. The alternatives, however, are also problematic:

As telecommunication systems grow through the deployment of advanced technology and the availability of service providers to access the network, so do the possibilities for liability. Protecting oneself against liability claims also becomes more complicated. Alternative approaches to liability protection must be developed. Because communication needs differ and those providing the services attempt to tailor services to meet consumer needs, every contract has the potential of being different. In such situations liability should be individually negotiated by contract. Alternatives to individually negotiated liability terms include attempting to develop a cookie-cutter approach to liability, or to rely on government regulation to protect against liability claims. These alternative approaches are least desirable in a deregulated telecommunications environment.

B. Fontes, *Liability and Interoperability Issues*, in INTERNATIONAL TELECOMMUNICATIONS UNION, REGULATORY SYMPOSIUM 40 (1991). Mr. Fontes is the Chief of Staff for the Federal Communications Commission.

<sup>1009</sup> Additionally, the extent to which the provision of enhanced security services is considered for regulation should be monitored. *See, e.g.*, Section VIII.G.1., *infra* (concerning telecommunications regulation).

## C. ESCROW AND OTHER LEGAL AGENTS

### 1. Escrow Agents

Escrow, trust and bailment relationships are similar to the FCA/certificate holder relationship in that the latter involves the entrusting and preservation of valuable and important items by and in the interest of the certificated holder. Examining the types of duties and liabilities associated with other trusted entity relationships will provide insight into the potential duties and liabilities of the FCA. If the duties of these other custodians correspond to those of the FCA, it will be required to exercise the requisite diligence and skill in performing those duties.

#### Duties and Liabilities of Escrow Agents

When a person assumes and acts as escrow agent, he is absolutely bound by the terms and conditions of the deposit and charged with strict execution of the duties he voluntarily assumed.<sup>1010</sup> The duties of an escrow holder have been determined by ordinary principles of agency.<sup>1011</sup> The escrow holder is a fiduciary and is required to exercise reasonable skill and ordinary diligence.<sup>1012</sup> In his fiduciary capacity, the escrow agent must perform his duties with scrupulous honesty, skill and diligence.<sup>1013</sup>

---

<sup>1010</sup> See 28 AM. JUR. 2D *Escrow* § 1, at 24 (1966); Annotation, 15 A.L.R. 2D 870 (1951).

<sup>1011</sup> See 28 AM. JUR. 2D, *supra* note 1010, § 1.

<sup>1012</sup> See 28 AM. JUR. 2D, *supra* note 1010, § 1, at 25.

<sup>1013</sup> See *id.* § 1. Certain laws mitigate the risks associated with dealing with fiduciaries. For example, the Utah Fiduciaries Act (UTAH CODE ANN. §§ 22-1-1 *et seq.*, 22-1-2, 22-1-9 (1953)) "facilitate[s] banking and financial transactions by giving relief from liability to those who deal with fiduciaries, except where they have knowledge that the fiduciary is breaching his duty to his principal, or knowledge of facts which would amount to bad faith as applied to dealing with the fiduciary. . . . Once [the Act] applies, there is a presumption of regularity as to the acts of the fiduciary, and the financial institution need not 'require a demonstration of authority.'" *Bridgeport Fireman's Ass'n v. Deseret Fed. S. & L.*, 633 F. Supp. 516, 521 (D. Utah 1986). The development of comparable laws appropriately reducing fiduciary risks to the FCA should be considered.



Liability attaches to the escrow agent if he or she improperly departs with the deposit,<sup>1014</sup> which constitutes a conversion.<sup>1015</sup> If an escrow agent violates instructions or acts negligently, he or she is ordinarily liable for any loss occasioned by the breach of duty.<sup>1016</sup>

### **Burden of Proof for Negligence of Escrow Agents**

In an action for negligence in handling an escrow, the burden is on the defendant escrow holder to demonstrate substantial compliance with the terms of the escrow agreement.<sup>1017</sup>

### **Relevant Escrow Agreement Clauses**

The following clauses are typical of the liability-related provisions that appear in commercial software escrow agreements. To the extent that they represent trade practice and usage, they provide useful insights for future FCA agreements.

**[Standard of Care]** "a professional level of care"

**[Indemnification]** Depositor agrees to defend and indemnify escrow agent and hold escrow agent harmless from and against any and all claims, actions and suits, whether in contract or in tort, and from and against any and all liabilities, losses, damages, costs, charges, penalties, counsel fees, and other expenses of any nature . . . incurred as a result of performance of the Agreement except in the event of a judgment which specifies that escrow agent acted with gross negligence or willful misconduct.

**[Reliance on Instructions]** Escrow agent may act in reliance upon any written instruction, instrument, or signature believed to be genuine and may assume that any person giving any written notice, request, advice or instruction in connection with or relating to the Agreement has been duly authorized to do so. Escrow agent is not responsible for failure to fulfill its obligations under the Agreement due to causes beyond its control.

---

<sup>1014</sup> See 28 AM. JUR. 2D, *supra* note 1010, § 1; see also *Citizens' Nat'l Bank v. Davisson*, 229 U.S. 215 (1913).

<sup>1015</sup> See 28 AM. JUR. 2D, *supra* note 1010, § 1, at 27.

<sup>1016</sup> See *id.* § 1.

<sup>1017</sup> See *id.* at 56.

[Audit Rights] Escrow agent agrees to keep records of the activities undertaken and materials prepared pursuant to the agreement. Upon normal notice, depositor is entitled to inspect the records.<sup>1018</sup>

The North American Securities Administrator's Association, Inc. (NASAA) Model Security Escrow Agreement for the release of stock certificates and shares contains presumptions concerning the performance of escrow agents thereunder that are also useful in considering some of the activities of an FCA:

9. The Escrow Agent may conclusively rely on, and shall be protected, when it acts in good faith upon, any statement, certificate, notice, request, consent, order or other document which it believes to be genuine and which has been signed by the proper party. The Escrow Agent shall have no duty or liability to verify such statement, certificate, notice, request, consent, order or other document and its sole responsibility shall be to act only as expressly set forth in this Agreement. The Escrow Agent shall be under no obligation to institute or defend any action, suit or proceeding in connection with this agreement unless it is indemnified to its satisfaction. The Escrow Agent may consult counsel in respect of any question arising under this Agreement and the Escrow Agent shall not be liable for any action taken, or omitted, in good faith upon advice of such counsel. All Shares held pursuant to this Agreement shall constitute trust property and the Escrow Agent shall not be liable for any interest thereon.<sup>1019</sup>

## 2. Trustee and Trustor Relationship

In a strict sense, a *trustee* is one "who holds the legal title to property for the benefit of another."<sup>1020</sup> However, the term is also used in a broader sense which it applies to anyone standing in a fiduciary or confidential relation to another, such as an agent, attorney, bailee, or the like.<sup>1021</sup>

---

<sup>1018</sup> Data Sec. Int'l, Preferred Registration Technology Escrow Agreement § 6 (1993).

<sup>1019</sup> H. BLOOMENTHAL, SECURITIES AND FEDERAL CORPORATE LAW app. § 14.14 (1972).

<sup>1020</sup> State *ex rel.* Lee v. Sartorius, 130 S.W.2d 547, 549-50 (1939); see BLACK'S LAW DICTIONARY 1508-09 (6th ed. 1990).

<sup>1021</sup> See BLACK'S LAW DICTIONARY 1508-09. Benjamin Cardoso described fiduciary duty in these terms: "[n]ot honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior." *Meinhard v. Salmon*, 249 N.Y. 458, 464 (1920). Cf. U.C.C. § 3-307(a)(1) (Notice of Breach of Fiduciary Duty) (defining "fiduciary" as "an agent, trustee, partner, corporate officer or director, or other representative owing a fiduciary duty with respect to an instrument."); the UNIF. FIDUCIARIES ACT § 1(1), 7A U.L.A. 395-96 (1985) (defining fiduciary).



## Duties and Liabilities of Trustees

The trustee owes a fiduciary duty to the beneficiary.<sup>1022</sup> The trustee must use due care, diligence, and skill with respect to the preservation and investment of trust property.<sup>1023</sup> A breach of this duty gives rise to liability and a correlative cause of action on the part of the beneficiary for any loss incurred.<sup>1024</sup> A trustee's liability for breach is personal in character. Accordingly, a trustee may be required to use his or her own resources to replenish the loss.<sup>1025</sup>

## Burden of Proof

The burden of proving the existence of a trust is on the party asserting its existence.<sup>1026</sup> When a beneficiary brings an action charging a trustee with a breach of trust, the beneficiary has the burden of proving in what respects the trust was breached.<sup>1027</sup> Additionally, the beneficiary has the initial burden of proving the existence of a fiduciary duty and the trustee's failure to perform it.<sup>1028</sup>

After the beneficiary has met this burden, the burden shifts to the trustee to justify its actions.<sup>1029</sup> The trustee must demonstrate the use of due care, diligence and skill.<sup>1030</sup>

---

<sup>1022</sup> See *Reinecke v. Smith*, 289 U.S. 172 (1933); BLACK'S LAW DICTIONARY 1514; 76 AM. JUR. 2D *Trusts* § 688, at 675 (1992).

<sup>1023</sup> See 76 AM. JUR. 2D., *supra* note 1022, at 675.

<sup>1024</sup> See *id.* at 363.

<sup>1025</sup> See *id.*

<sup>1026</sup> See *id.*

<sup>1027</sup> See *id.*

<sup>1028</sup> See *id.*

<sup>1029</sup> See *id.*

<sup>1030</sup> See *id.* at 675-76.

### 3. Bailor - Bailee Relationship

"A bailment is a delivery of goods or personal property, by one person [the 'bailor'] to another [the 'bailee']" for the use, care or execution of a special task relating to the goods and then "either to redeliver . . . or otherwise dispose" of them in accordance with the bailment.<sup>1031</sup>

#### Duties and Liabilities of Bailees

The bailee is responsible for exercising due care toward the goods.<sup>1032</sup> However, no fiduciary or trust-beneficiary relationship is created.<sup>1033</sup> The duty of care or exercise of skill will vary by the terms of the particular bailment.<sup>1034</sup> Thus, when a bailment is for the benefit *only* of the bailor (*i.e.*, an uncompensated holding for the bailor's benefit), the bailee need exercise only slight diligence. When the bailment is for the benefit only of the *bailee* (*i.e.*, a gratuitous loan), the bailee will be liable for even slight negligence. Finally, when the bailment is for the benefit of both parties (*e.g.*, loan for hire or pledge), ordinary due care is the standard.<sup>1035</sup>

The federal government has been held liable under the Federal Tort Claims Act and the Tucker Act for the negligent loss of goods held by the government as bailee.<sup>1036</sup>

#### Burden of Proof for Negligence of Bailee

A bailee who has sole, actual and exclusive physical possession of the goods is presumed to be negligent if he or she cannot explain the loss or disappearance of

---

<sup>1031</sup> BLACK'S LAW DICTIONARY 179.

<sup>1032</sup> *See id.* at 142.

<sup>1033</sup> *See id.*

<sup>1034</sup> *See* 8 AM. JUR. 2D *Bailments* § 131, at 860 (1980).

<sup>1035</sup> *See* 1 BOUVIER'S LAW DICTIONARY 313-14 ("Bailment") (3rd rev. 1914).

<sup>1036</sup> *See, e.g.*, *Alliance Assurance Co., Ltd. v. United States*, 252 F.2d 529 (2d Cir. 1958); *see also* Sections VII.A.3.b. ("The Tucker Act"); VII.A.3.a. ("Federal Tort Claims Act"), *supra*.



the goods, and the law imposes on him or her the burden of showing that he or she exercised reasonable care.<sup>1037</sup>

#### **4. Insurance Agent-Insured**

The status of the relationship between an insurance broker and the insured is, in part, a function of the type of insurance agent involved: varieties include soliciting agents, special agents and general agents.<sup>1038</sup> However, "so long as the general rule prevails that an agent may not serve two principals simultaneously, it seems clear that in most contexts there is more justification for treating a broker as an agent of an insurer than as an agent of the insured."<sup>1039</sup>

#### **Burden of Proof for Insurance Agent**

"The standard of reasonable care by which [an insurance sales representative] intermediary is judged is usually that of a prudent person possessing the expert knowledge that the intermediary has or represents himself or herself as having, whichever is greater."<sup>1040</sup>

#### **5. Vault & Safe Deposit Boxes**

This subsection considers the warranties and apportionment of liability provided in standard agreements offered by commercial safe deposit/vault manufacturers and service providers. The companies are selling security and assurances, and therefore offer parallels to certain potential services of the FCA.

Customer-bank agreements for the lease of a safe deposit box are typically highly exculpatory in favor of the bank. The following clause provides an example of such terms:

The Lessee assumes all risks and liabilities arising from the use of the safe deposit box and retains responsibility for any loss, destruction, or damage of the contents of such safe

---

<sup>1037</sup> See 8 AM. JUR. 2D, *supra* note 1034, § 325, at 1059-60; *United States v. Cloverleaf Cold Storage Co.*, 286 F. Supp. 680 (N.D. Iowa 1968).

<sup>1038</sup> See KEETON & WIDISS, *supra* note 16, § 2.5, at 83.

<sup>1039</sup> *Id.* at 83-84.

<sup>1040</sup> *Id.* at 97 (citing *Fiorentino v. Travelers Ins. Co.*, 448 F. Supp. 1364, 1369-70 (E.D. Pa. 1978)).

deposit box. It is the sole responsibility of the Lessee(s) to obtain insurance on the contents of the safe deposit box. The Bank shall exercise ordinary diligence so that unauthorized persons may not be allowed access, and shall further exercise ordinary diligence so that fire, flood and other natural disasters be prevented from destroying or damaging the contents of such safe deposit box, but this shall be the limit of the Bank's responsibility. Mere proof of partial or total loss of the contents of any leased safe deposit box shall not be evidence of unauthorized access or failure of the Bank to exercise ordinary care. Further, the Bank's liability shall not exceed in any event the amount set forth in Act No. 319, Public Acts of 1969 of the State of Michigan.<sup>1041</sup>

## D. NOTARIES PUBLIC

### 1. Introduction

This section considers the FCA-relevant attributes of notaries public.<sup>1042</sup> In many respects, notaries public provide an important conventional analog to various proposed FCA duties and services. For example, both notaries public and the FCA can provide forms of time and date stamping, retention of a *record copy* or digest of a transaction for dispute resolution purposes, maintenance of transaction logs, and assurances respecting users' signatures (including, in the case of the FCA, digital signatures). However, when notaries are "force-fitted" to support computer-based processes and practices, they embark upon a dangerous collision course with the law.<sup>1043</sup>

### 2. Applications and Relevance

Despite legal barriers to computer-based notarial acts, there are three FCA-relevant functional areas in particular that could benefit either from the existing notarial infrastructure or, to a degree, from a future notarial infrastructure. These functional areas are intended to: (a) support a trustworthy *remote* FCA user-application process,<sup>1044</sup> (b) support enhanced FCA user-application process via

---

<sup>1041</sup> Comerica Bank Safe Deposit Terms (current as of 1992).

<sup>1042</sup> See Appendix C, *infra* (surveys the law of notaries public and provides an overview of certain law pertinent to their automation).

<sup>1043</sup> As an institution of the conventional paper world, notaries public encounter legal disabilities when confronted with modern technology, such as prohibitions against acknowledging information in computer-based form, including electronic mail or EDI documents.

<sup>1044</sup> See Section VIII.D.2.a., *infra*.



*internal* FCA notaries,<sup>1045</sup> and (c) provide a model for FCA administrative conduct and procedures. Each of these areas is discussed below.

#### a. "Remote" FCA Notaries

Notaries public present possible approaches to facilitating the certificate application process in a trustworthy fashion. One particular benefit of utilizing notaries public is to satisfy possible FCA *personal presence* certificate application requirements. There are more than four million notaries public; they are: (i) geographically highly distributed (thereby providing a cost-effective and logistically practical institution), (ii) commissioned officers of state governments (thereby, perhaps, enhancing the legal efficacy of the certification), and (iii) already vested with special government-sanctioned powers to acknowledge documents,<sup>1046</sup> and to perform verifications.<sup>1047</sup>

Moreover, the performance of identification assurance procedures by a pre-existing, national network of notaries would permit the FCA to remain highly centralized. Centralization would be cost effective and logistically advantageous, at least during the early stages of FCA development, piloting and implementation. One scenario in which the notary public can support a centralized FCA infrastructure by *remotely* evaluating user-applications is described in the following figure.<sup>1048</sup>

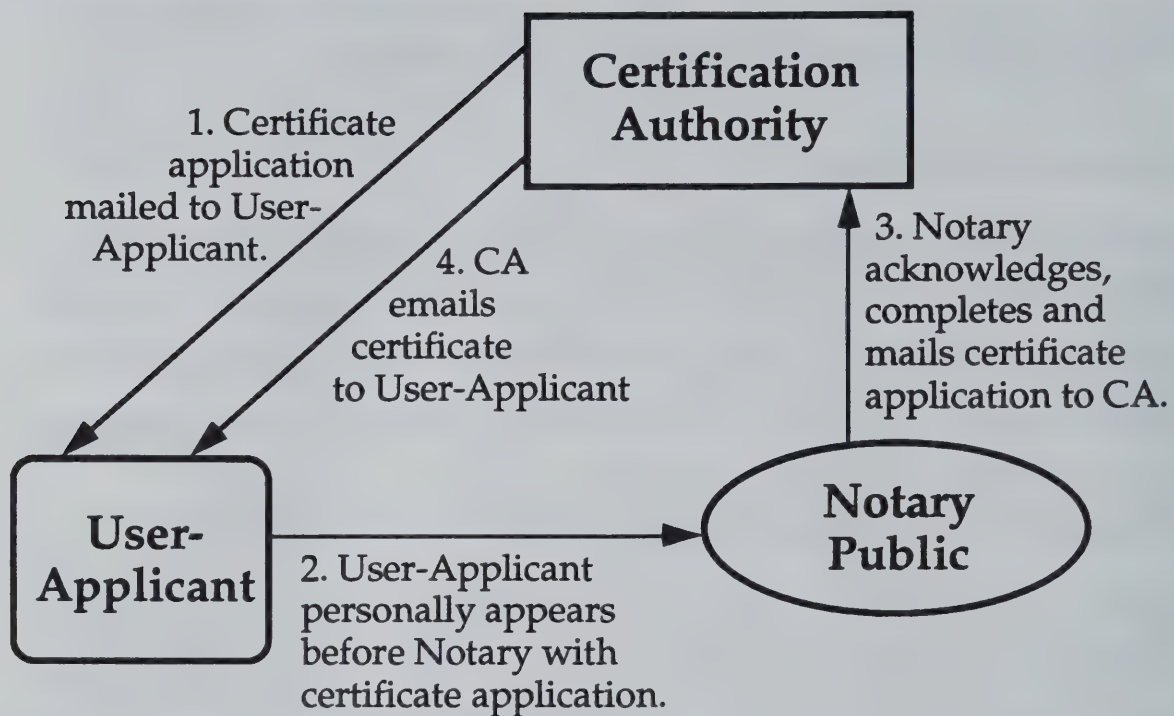
---

<sup>1045</sup> See Section VIII.D.2.b., *infra*.

<sup>1046</sup> A certificate of acknowledgment is signed by "a notary public, justice of the peace, or other authorized officer, attached to the deed, mortgage, or other instrument, and sets forth that the parties thereto personally appeared before him on such a date and acknowledged the instrument to be their free and voluntary act and deed." BLACK'S LAW DICTIONARY 286. An acknowledgment authenticates the instrument; permits the instrument to be introduced into evidence without proof of execution; and entitles the instrument to be recorded. See 1 AM. JUR. 2D *Acknowledgments* § 4.

<sup>1047</sup> A verification is a sworn statement as to the truth of the facts stated within the instrument. See 1A C.J.S. *Acknowledgments* § 2 (1985).

<sup>1048</sup> This scenario is described in ELECTRONIC CONTRACTING, *supra* note 2, at 216; see also Appendix D., *infra* (exhibiting the form used to accomplish remote certificate application processing by RSA Certificate Services.).



**FIGURE 1 - NOTARY FACILITATION OF REMOTE CERTIFICATE APPLICATION PROCESS**

Advocates for the performance of FCA services by the U.S. Postal Service likewise contend that post offices are highly distributed, with customer-accessible locations throughout the United States, and that the USPS is therefore suitable for the support of personal appearance requirements for applicants before a federal agent (*i.e.*, a postal clerk or the local postmaster) for identification, credential-certificate binding and FCA administrative purposes.<sup>1049</sup> However, notarial and USPS roles and services are not necessarily mutually exclusive, as explained in the next subsection.

#### **b. Notaries Internal to the CA**

Another scenario places the notary public *inside* the certification authority. The internal notary public provides the same functions that it provides in its remote role except that it is associated formally, physically and administratively with the FCA. The following figure exemplifies this scenario:

<sup>1049</sup> See Section VII.A.4.a., *supra* (considering the USPS as an FCA provider).



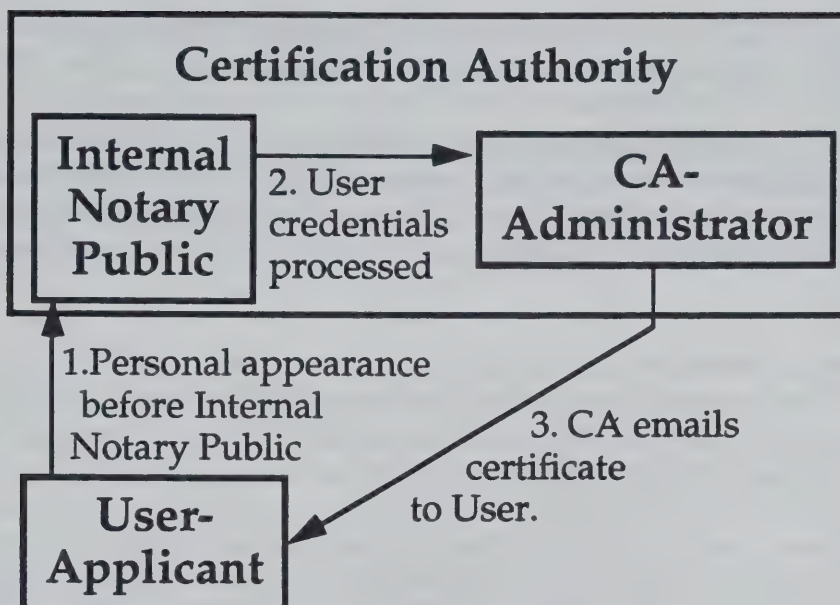


FIGURE 2 - NOTARY INTERNAL TO CERTIFICATION AUTHORITY

The critical issue here is whether the notary, as a matter of both law and public perception, operates with a desirable level of independence, in that the greatest barrier to internal notary viability concerns whether the internal notary will be characterized as holding a *disqualifying interest*.<sup>1050</sup>

### 3. Notarial Independence; Disqualifying Interests

Case law does not preemptively find a disqualifying interest when, for example, the notary does not have a direct interest in the instrument. However, there is fear, particularly within circles arguing for the so-called *super notary*,<sup>1051</sup> that the notary public must be unequivocally independent and therefore cannot operate within a certification authority.<sup>1052</sup> Moreover, to the extent that the notary's acts

<sup>1050</sup> The problem is explored below in Section VIII.D.4.

<sup>1051</sup> See Section VIII.D.6., *infra*. This expression was coined by the author for want of a better term to describe *something better* than that provided by American-styled common law notaries and yet distinct from the scope and powers of the Latin notary. The term "cybernotary" was subsequently adopted (at least tentatively) by members of the ABA's Information Security Committee at its April 1994 meeting.

<sup>1052</sup> Cf. Figure 1, *supra*, and accompanying text.

will include *quasi-judicial* acknowledgments, such acts, although not "strictly judicial, [are] of a judicial nature and require[] disinterested fidelity."<sup>1053</sup>

The impact of a disqualifying interest may extend beyond liability for the notary and affect the validity of the acknowledged document. In the extreme, a disqualifying interest could invalidate all digital signatures created pursuant to corresponding notarially acknowledged or verified certificate user-applications (CRD).

In a recent case, an attorney acted in the dual role of notary and trustee under a deed of trust.<sup>1054</sup> The court recognized that some jurisdictions had adopted a *per se* rule holding documents void upon a finding of interest, but instead decided to adopt a rule that would not avoid transactions based on interest alone:

. . . where there is no imputation or charge of improper conduct, bad faith, or undue advantage, the mere fact that the acknowledgment was taken before an interested officer will not vitiate the ceremony or render it void if it is otherwise free from objection or criticism. The fact of interest, however, ought to be regarded with suspicion and should provoke vigilance to detect the presence of unfair dealing, the slightest appearance of which the party seeking to uphold the acknowledgment should be required to clear away.<sup>1055</sup>

The court continued,

Thus, we conclude that once it is shown that a notary has a disqualifying interest in an instrument which he acknowledged, and a suggestion of actual prejudice, unfair dealing, or undue advantage is raised by an adverse party, then the burden shifts to the notary or any party seeking to support the challenged document to demonstrate that no improper benefit was obtained and no harm occurred as a result of the disqualified act.<sup>1056</sup>

---

<sup>1053</sup> *Stevens v. Hampton*, 45 Mo. 404, 407 (1870) (cited in *Galloway v. Cinello*, 423 S.E.2d 875, 878 (W. Va. 1992)).

<sup>1054</sup> *See Galloway*, 423 S.E.2d at 877 ("[T]he bankruptcy trustee filed a complaint in the bankruptcy court alleging that Ms. Cinello did not have a perfected lien on the real estate because Mr. Galloway, as the trustee in the deed of trust, had also acknowledged the signatures of the [grantors].").

<sup>1055</sup> *Id.* at 879 (quoting 1 AM. JUR. 2D *Acknowledgments* § 16 at 458-59).

<sup>1056</sup> *Id.* at 880.



#### 4. Model for FCA Conduct and Procedures?

The notary public contributes to a model for FCA administrative conduct and procedures. As a legally recognized trusted entity, the institution of the notary public provides a rich set of structures upon which the FCA can build a foundation. Appendix C ("Automation of the Notary Public") hereto identifies many of these structures and explores their relationship to computer-based practices.

#### 5. Liability

The liability of notaries public for negligent or intentional misconduct varies among the states. However, as a general matter, "[t]he duty of a notary public in acting officially is not confined to the public and those who may be affected by his act. The public has a right to rely on the verity of a certificate . . . . It is not necessary that the wrongful act of the notary shall be the sole cause of the loss. If it is a concurring cause and plays a part in bringing about the injury, the liability for the loss is fixed."<sup>1057</sup> As the court in *Galloway v. Cinello* noted,

[E]ven in the absence of any specific statutory language, courts have held a notary and his official surety civilly liable for negligence in the performance of notarial duties. The most frequent causes are those where the notary has acknowledged a deed or other instrument without ensuring that the person whose signature he acknowledged was in fact the person he or she was represented to be. . . . The standard is no longer limited to corrupt or malicious acts on the part of a notary . . . negligence will suffice to create liability.<sup>1058</sup>

The existence of statutorily required bonds in a minimum amount for notaries public in certain states should be noted. A similar concept is fairly likely for any government sponsored, civilly liable notary public in the FCA context.

---

<sup>1057</sup> *American Sur. Corp. v. Boden*, 50 S.W.2d 10 (Ky. 1932).

<sup>1058</sup> *Galloway*, 423 S.E.2d at 880-81.

Note that the Latin style notaries' liability is typically considerable. If a notary, in the exercise of his/her notarial office causes any loss through negligence or bad faith to any person who has relied on his/her professional office, such notary is obliged to indemnify that person for the loss suffered. Commission of Int'l Notarial Cooperation, *Guidelines on Fundamental Principles of the Latin Notariat System* art. 11 (Hague, 1986).

## 6. Notarial Law Reform

Notarial law reform efforts should be monitored by all parties interested in FCA development. The primary international body that has expressed interest in notarial reform to accommodate computer-based practices is the International Union of Latin Notaries.<sup>1059</sup> Additionally, the Hague Conference has informally expressed interest in notarial reform in the context of possible reform of the Hague Convention Abolishing the Requirements of Legalization for Foreign Public Documents.<sup>1060</sup>

The Nonrepudiation and Notarization Work Group within the American Bar Association's Information Security Committee (the "Notarization Work Group")<sup>1061</sup> has commenced notarial reform initiatives. The Notarization Work Group is studying the roles and requirements for notaries public in a computer-based world. Comprised of U.S. and foreign notaries public associations; government and private lawyers; and information, MIS and security systems managers, it recognizes that conventional (American-style) notaries public cannot fulfill the diverse and novel demands created by computer-based information due to (real or perceived) inadequate trustworthiness and competence. Consequently, the Notarization Work Group is developing proposed ABA resolutions which address the legal standing of notaries within the context of supporting certification authority entities, and evaluate the propriety of revision to the

---

<sup>1059</sup> The President of the Luxembourg-based Union has informally stated that cooperation and action among the Union and the United States to upgrade U.S. notaries and thereby permit U.S. entry into the Union is his "highest priority." He also noted the likelihood of the Union adopting English as one of its official languages. Interview with A. Schwachtgen, President, Union Internationale Du Notariat Latin, in Vienna Oct. 16, 1993). The Union has also demonstrated its commitment to the reform process by active participation within the Notarization Work Group. See note 1061, *infra*.

<sup>1060</sup> Done at the Hague, Oct. 5, 1961 and entered into force for the United States on Oct. 15, 1981. The Hague Convention has been endorsed by the American Bar Association and the U.S. Department of Justice. The convention eliminates "requirements of proving a chain of authentication with the final diplomatic signature among member states" ELECTRONIC CONTRACTING, *supra* note 2, at 210.

<sup>1061</sup> The Information Security Committee sits within the EDI and Information Technology Division, Section of Science and Technology. Another of the Committee's work groups, the Certification Authority Work Group, is developing "Global Public Key Infrastructure Rules of Practice and Commentary" and also considering requirements for legislative reform potentially needed to support a viable certification infrastructure. See Section IX.D.1, *infra*.



Hague Convention<sup>1062</sup> and undertaking other notarial projects in support of computer-based trustworthiness.

Notarial law reform in support of public key infrastructure is poised to receive greater attention both domestically and internationally<sup>1063</sup> as the importance of trusted entities in support of certificate-based public key and other information security services becomes better appreciated.

## 7. The Case for the "Super Notary"

Recognizing the need for assurances of trust, particularly in computer-based practices, there is a small but growing group of proponents for the development of either a new class of notaries, *super notaries* (or *cybernotaries*), or some new institution of computer-literate, highly trusted professionals whose role would involve the facilitation of diverse trust functions in a secure computer-based infrastructure.<sup>1064</sup> In one scenario, the super notary class would be a peculiarly American institution because ordinary notaries are less trained, less educated, and

---

<sup>1062</sup> See Information Sec. Committee, Section of Science and Technology, ABA, *Preliminary Report, Compilation of Results and Analysis of Responses to the Questionnaire on The Hague Convention Abolishing the Requirements of Legalization for Foreign Public Documents* (1993).

<sup>1063</sup> For example, "The Québec Board of Notaries has already undertaken the necessary procedures to have its constituent laws adapted to computer-based notarization [adopting 5s] and to enable its members to assume these new roles." C. Perrault, Notary, *Chambre des Notaires du Québec, Toward Computer-Based Notarization in the Province of Québec* 9 (Notarization Work Group, 1993). See Hawkes and Montijn, *Trusted Third Parties and Similar Services*, Final Report (TEDIS, Sept. 1991).

<sup>1064</sup> "By this time I think most will agree that the notaries in the United States are not ready to assume the role of trusted entities without further selection, education and training." E. Hines, *Credentialing EDI Trusted Entities* 2 (Notarization Work Group). Compare the following: "Needs for a new class of notaries or for Trusted Entities are not felt in the province of Québec for, on the one hand, notaries already possess all of the necessary attributes to accommodate computer-based notarization and, on the other hand, the Québec Board of Notaries already acts as a government appointed trusted entity." Perreault, *supra* note 1063, at 9.

less trusted<sup>1065</sup> than their name-sakes in civil law countries.<sup>1066</sup> The super notary might have the following qualifications:

- a. Attorney - licensed to practice law in the United States. Malpractice insurance might also be required.
- b. Notary Public - registered under current law within the United States. A comparatively large surety bond might also be required.

---

<sup>1065</sup> See Appendix C *infra* (discussing fallibilities and distrust of the American notary public).

<sup>1066</sup> The civil or Latin law notary is a qualified attorney who has trained, passed special notarial examinations and been admitted to the notarial profession. Notaries, such as those in Québec, France, or Italy, are permitted to act as legal advisors, prepare documents and appear before court in non-contested matters. The Latin law notary entails:

- ascertainment of the personal identity of the appearing parties;
- ascertainment of the powers of the contracting parties to negotiate;
- inquiring into the will of the parties;
- interpretation of the will of the parties;
- verification of the parties' freedom and autonomous expression of will;
- verification of the availability of the subject matter of the contract;
- examination of the conformity of the parties' will with the legal system principles to be observed;
- conversion of the contractual will into written work having a clear, simple and incontrovertible juridical significance;
- drawing-up of the document in a correct juridical form, substantially and formally appropriate for achievement of the parties' purpose;
- adaptation of the parties' will to the economic, juridical and social systems so that such will may be executed within the limits of the juridical system, also by means of legal publicity, with consequent safeguarding of the juridical system itself;
- attribution of public faith to the deed, in both public and private interest, so as to meet the citizen's desire for security;
- counselor service for the parties;
- preservation of professional autonomy.

Comité Franco-Italien Du Notariat Ligure Et Provençal, *The Function of the Latin Law Notary*, Hommage au XiX<sup>e</sup> Congrès Internationale du Notariat Latin, Amsterdam (1989).



c. Independent - unbiased; self-employed or not employed by any entity other than a law firm or government instrumentality.

d. Certification of Computer Literacy - required to take an examination and be certified by a designated accrediting entity.<sup>1067</sup> The certification would attest to the super notary's knowledge and skill to create, review, communicate, retain and digitally sign and verify computer-based information.

These criteria, among others, are under consideration within the Working Group.

## E. CHAMBERS OF COMMERCE

"Chambers of Commerce" play important trusted roles for the facilitation of trade and business, particularly at the international level in respect of the International Bureau of Chambers of Commerce (the "IBCC") of the International Chamber of Commerce ("ICC"). Three initiatives of the IBCC or its national affiliates may provide structures and procedures relevant to the FCA: CEDI-FACT, ATA Carnet, and the Certificate of Origin. Each of these initiatives is intended to provide business assurances based upon the real and perceived trustworthiness of the Chambers as bolstered by formal mechanisms for compensatory relief, as discussed below.

### 1. CEDI-FACT / FAST

The IBCC, world forum of Chambers of Commerce (of the ICC),<sup>1068</sup> is establishing an international "registration" and "certification" chain for EDI assurances.

---

<sup>1067</sup> See generally Section IX.A. ("Certification and Accreditation"), *infra*. A proposed resolution under consideration and further development within the Information Security Committee provides:

BE IT RESOLVED THAT the Section of Science and Technology supports in principle the creation of an entity to provide specialty certification of attorney-notaries [electronic transaction specialists] engaged in the professional services related to transnational electronic commerce.

B. Cottine, Co-Chair, Legislation and Resolutions Committee, Sect. of Science and Technology, ABA, Memorandum to Section Officers and Council Members (February 3, 1994).

<sup>1068</sup> "Founded in 1919, the ICC is the world business organization; it is unique in being the only business representative body whose membership is both

Coordinated by the Belgian Federation of Chambers of Commerce and Industry, the backbone of the Certified Electronic Data Interchange For Administration, Commerce and Transport ("CEDI-FACT") concept is "FAST" (First Attempt to Secure Trade), a trans-European and trans-sectoral pilot project started in December 1993 under the auspices of the TEDIS program<sup>1069</sup> of the Commission of the European Union. CEDI-FACT is intended to develop an infrastructure to facilitate "Chambers of Commerce and Industry and their National Organizations" in performing CA and "CCA" (central certification authority) roles.<sup>1070</sup> A CEDI-FACT project overview states, "we think that Chambers of Commerce and Industry can act as certification authorities . . . [because the characteristics of the Chambers<sup>1071</sup>] are widely recognized by the business community and constitute the main qualities requested from a real 'trusted third party'."<sup>1072</sup>

---

worldwide and multisectoral. As such, the ICC enjoys the highest consultative status with the UN system, and close working relations with the GATT, World Bank, IMF, OECD and EC. Its international headquarters, with a multinational staff, is based in Paris, and its membership extends to 110 countries, the majority of which are in the developing world." D. Hascher, *Methods of Improved Coordination between Formulating Agencies: the International Chamber of Commerce (ICC)* (Uniform Commercial Law in the 21st Century, Congress organized by the UNCITRAL, 18-22 May, 1992, United Nations, New York).

<sup>1069</sup> See generally TEDIS, Trade EDI Systems Programme, Interim Report 1992. The TEDIS program of the Commission of the European Communities, Directorate-General XIII on Information Technologies and Industries, and Telecommunications, coordinates and launches EDI-relevant projects in various sectors of European Industry, including with respect to EDI registration authorities, information security, technology integration, interconnectivity and interoperability.

<sup>1070</sup> M. Peereman, *Project CEDIFACT 7* (paper presented at "New CCI Services to Enterprises," EUROPA '92, Nice, Dec. 10, 1992); see TEDIS, FAST (Oct. 1993).

<sup>1071</sup> These characteristics include: lack of profit motive; multi-sectoral organization; independence from public authorities, political parties and pressure groups; independence from commercial or industrial interest; recognized qualities of integrity and confidentiality; service orientation; involvement in education, information and guidance; coordination of international activities through their international CCI organizations; existing certification expertise and expertise with the ATA Carnet system. See Peereman, *supra* note 1070, tbl. 6.

<sup>1072</sup> *Id.* at 7.



## 2. ATA Carnet

Conventions have been established to allow for the temporary importation of different classifications of merchandise. An ATA Carnet (*admission temporaire*) is an international customs document which functions as a "merchandise passport" to facilitate temporary duty-free importation of commercial samples, professional equipment and goods for fairs and exhibitions. The Carnet is both an entry document and a guarantee of duty and tax payment. It eliminates certain customs procedures for temporary import, such as requirements of a deposit equal to duties and taxes subject to refund on departure, or purchase of a temporary import bond for the amount of duties and taxes which could become payable if the goods were sold or the terms of temporary importation were breached. The Carnet has been used to facilitate the transfer of over one billion dollars of merchandise, and its use continues to increase.

The ATA Carnet System is relevant to the FCA in that it certifies certain conditions<sup>1073</sup> and structures compensation for liability: the U.S. Council for International Business ("USCIB") relies on a combination of insurance,<sup>1074</sup> security,<sup>1075</sup> an equity fund maintained by the USCIB and liability apportionment provisions pursuant to contract between the USCIB and applicants.

Upon issuance,

1. Each guaranteeing association shall undertake to pay to the Customs authorities of the country in which it is established the amount of the import duties and any other sums payable in the event of non-compliance with the conditions of temporary admission or of transit . . . . It shall be liable jointly and severally with the persons from whom the sums mentioned above are due, for payment of such sums.

2. The liability of the guaranteeing association shall not exceed the amount of the import duties by more than ten percent.<sup>1076</sup>

---

<sup>1073</sup> Indeed, the ATA Carnet warranties may provide greater assurances than those contemplated by certain FCA entities.

<sup>1074</sup> "Catastrophic insurance coverage" is provided by insurers to the USCIB. See generally Section IX.B, *infra* (concerning insurance).

<sup>1075</sup> Forms of security include: cash deposits, letters of credit, third-party guarantees, bonds and written agreements deposited with the USCIB to indemnify it against any loss for payments it may be called upon to make on behalf of the carnet holder.

<sup>1076</sup> A.T.A. Convention, ch. IV, art. 6.

The ICC, working closely with the Customs Cooperation Council ("CCC"), administers the ATA Carnet System worldwide. Customs authorities in the participating countries accept carnets as a guarantee that all duties and excise taxes will be paid if any items covered by the carnet are not re-exported within the time period allowed by the importing countries. The USCIB was appointed by the U.S. Treasury Department to administer the ATA Carnet system in the U.S. In 1992, the USCIB issued 10,936 carnets.<sup>1077</sup>

### 3. Certificate of Origin

A *Certificate of Origin* provides assurances to customs authorities that identified goods originated in a specified country. The Certificate of Origin is issued by the shipper's local Chamber of Commerce. The Certificate of Origin's attestation clause, which is executed by the Chamber, reads as follows:

The [], a recognized Chamber of Commerce under the laws of the State of [], has examined the manufacturer's invoice or shipper's affidavit concerning the origin of the merchandise, and, according to the best of its knowledge and belief, finds that the products named originated in the United States of North [sic] America.<sup>1078</sup>

In the event of default, the issuing Chambers of Commerce is liable. Some Chambers of Commerce obtain insurance; others self-insure.<sup>1079</sup>

### F. DEPARTMENT OF STATE (PASSPORTS)

The Department of State serves as a trusted entity in its passport administration role. As the issuer of a "primary" identification document (one that is a close analog to a "national ID"), the Department of State's passport regulations

---

<sup>1077</sup> See USCIB, Annual Report: 1992-1993.

<sup>1078</sup> Form 1208, Hobbs & Warren, Inc., Boston. Cf. North American Free Trade Agreement Certificate of Origin, Form CF 434 (Dec. 30, 1993) (providing self-certification).

<sup>1079</sup> See Section IX.B., *infra* (concerning insurance); cf. Customs Modernization Act of 1993, Title VI, Pub. L. No. 103-182 (1993), art. 501 *et seq.* (establishing a Certificate of Origin by the exporter without "third party" intervention such as by a Chamber of Commerce). See Section VII.A.4.e. ("Other Domestic Entities"), *supra*.



(particularly those regulations addressing proof of identity) deserve scrutiny by the FCA.<sup>1080</sup> A *passport* is "any travel document issued by competent authority showing the bearer's origin, identity, and nationality if any, which is valid for the entry of the bearer into a foreign country."<sup>1081</sup> Passports are official government documents and remain the property of the federal government.<sup>1082</sup> A passport identifies a citizen,<sup>1083</sup> and certifies that the subject is a U.S. citizen and requests foreign powers "to permit the citizen/national of the United States named [therein] to pass without delay or hindrance and in the case of need to give all lawful aid and protection."<sup>1084</sup>

**Application for passport:** The Secretary of State may grant and issue passports.<sup>1085</sup> An applicant must submit a written application, and if not previously issued a U.S. passport, "the application shall be duly verified by his oath before a person authorized and empowered by the Secretary of State to administer oaths."<sup>1086</sup>

---

<sup>1080</sup> See generally Section V.B. ("Certificate Application Process"), *supra*.

<sup>1081</sup> 8 U.S.C. § 1101(a)(30); cf. 22 C.F.R. § 50.1(e) ("attesting to the identity and nationality of the bearer").

<sup>1082</sup> See *Lynd v. Rusk*, 389 F.2d 940 (D.C. Cir. 1967); 22 C.F.R. § 51.9. (must be returned upon demand to the government).

<sup>1083</sup> See *United States v. Laub*, 385 U.S. 475 (1967).

<sup>1084</sup> The quoted language appears in all United States passports.

<sup>1085</sup> See 22 U.S.C. § 221a. Such authority is designated without requiring approval or ratification of the President. See Exec. Order No. 11295 (Aug. 5, 1966), 31 Fed. Reg. 10603 (Rules Governing Granting, Issuing, and Verifying of Passports). This delegation of power permits the Secretary to make reasonable classifications of persons to be granted or denied passports. See *Boudin v. Dulles*, 136 F. Supp. 218 (D.D.C. 1955).

<sup>1086</sup> 22 U.S.C. § 213; 22 C.F.R. § 51.21(a). The persons authorized by the Secretary of State to give oaths for passport purposes are:

- (1) A passport agent;
- (2) A clerk of any Federal Court;
- (3) A clerk of any State court of record or a judge or clerk of any probate court;
- (4) A postal employee designated by the postmaster at a post office which has been selected to accept passport applications;
- (5) A U.S. citizen employee of the Department of Defense designated by the Secretary of Defense to accept passport applications at a military installation within the continental United States selected to accept passport applications;
- (6) A diplomatic or consular officer abroad; or

Persons who have previously received a passport can renew the passport without personal presence upon completing an application.<sup>1087</sup>

**Evidence of U.S. Citizenship:** A "[b]irth certificate under the seal of the official custodian of birth records"<sup>1088</sup> is considered primary evidence. The "best obtainable secondary evidence" may be substituted for primary evidence when primary evidence is not available.<sup>1089</sup>

The passport office may require "additional evidence of identity as may be deemed necessary,"<sup>1090</sup> and may retain evidence when it is deemed necessary.<sup>1091</sup> Information in passport files is privileged and release of such information is restricted.<sup>1092</sup>

**False Statements:** The statute prohibiting the willful and knowing making of false statements in passport applications requires specific intent only to misstate information on a passport application rather than specific intent to defraud.<sup>1093</sup>

---

(7) Any other person specifically designated by the Secretary.

22 C.F.R. § 51.21.

<sup>1087</sup> The previous passport, two recent photographs, and the fee must be enclosed. 22 C.F.R. § 51.21(c).

<sup>1088</sup> *Id.* § 51.43(a).

<sup>1089</sup> *Id.* Secondary evidence includes "baptismal certificates, certificates of circumcision, or other documentary evidence created shortly after birth but not more than 5 years after birth, and/or affidavits of persons having personal knowledge of the facts of the birth." *Id.*

<sup>1090</sup> *Id.* § 51.28(c).

<sup>1091</sup> *See id.* § 51.55.

<sup>1092</sup> *See id.* § 51.33.

<sup>1093</sup> *See* Liss v. United States, 915 F.2d 287 (7th Cir. 1990); *see also* 18 U.S.C. § 1542 (false statement in passport); *cf.* 18 U.S.C. § 1717 (use of postal service as a conduit to make false statements); Sections VI.C.2.b.-c., *supra* (concerning misrepresentation).



**Validity:** A passport is valid for ten years from date of issue, unless otherwise restricted.<sup>1094</sup> A passport represents proof of citizenship.<sup>1095</sup> It is only valid when signed by the bearer,<sup>1096</sup> and may be verified at the request of the bearer or a foreign government.<sup>1097</sup>

**Denial and Revocation of Passport:** The passport regulations include a list of circumstances that permit the denial of passports, including when the applicant is subject to an outstanding federal warrant, criminal court order, request for extradition, or subpoena concerning a grand jury investigation of a felony, or has been declared incompetent or threatens serious damage to national security.<sup>1098</sup> The denial or revocation of a passport requires the exercise of due process, particularly when it affects personal liberty and property,<sup>1099</sup> and even when there is a likelihood of severe damage to national security or foreign policy.<sup>1100</sup>

### G. COMMON CARRIERS

One might tentatively define common carriers as entities engaged in certain lines of business which the law subjects to special rules as a result of their market power or other inability on the part of customers to control or monitor their activities.<sup>1101</sup> Examples of common carriers, so defined, include broadcasters,

---

<sup>1094</sup> See 22 U.S.C. § 217a.

<sup>1095</sup> See *id.* § 2705 (passports have "same force and effect as certificates of naturalization or citizenship issued by the Attorney General or by a court having naturalization jurisdiction").

<sup>1096</sup> See *id.* § 51.4.

<sup>1097</sup> See *id.* § 51.7.

<sup>1098</sup> See *id.* § 51.70; *cf.* Sections IV.G. ("Privilege"); V.B.3.-4., *supra* (concerning constraints on certificate issuance).

<sup>1099</sup> See *Boudin v. Dulles*, 136 F. Supp. 218 (D.D.C. 1955).

<sup>1100</sup> See *Haig v. Agee*, 453 U.S. 280 (1981); *cf.* Section V.D. ("Certificate Revocation"), *supra*.

<sup>1101</sup> *Cf.* United States Shipping Act of 1984, 46 U.S.C. App. § 1702(6). Professor Kozolchyk states that "the term 'carrier' seems to have been coined in Anglo-American legal discourse largely to aid in the assessment of liability for damage to cargo." Kozolchyk, *supra* note 26, at 178.

railroads, warehousemen and public utilities. During and prior to the nineteenth century, these special rules took the form of particularized liability rules;<sup>1102</sup> the twentieth century has typically seen the advent of pervasive regulatory schemes which may or may not address the subject of liability.

Because it has been suggested above that the FCA might be constituted as, or be deemed to be, a common carrier, this section examines the Federal Communications Commission (the "FCC") in its role as regulator of communications common carriers, which perform services that are comparable to certain anticipated FCA services.<sup>1103</sup> To provide further context, this section also surveys liability regimes that have been instituted to cover similar activities abroad and loss or injury to goods in transit. Although differences in the value of the "matter" being transported cause the latter regimes to have little *direct* relevance to FCA activities, their liability allocations are instructive, particularly where consequential damages become an important facet of the FCA's liability regime.<sup>1104</sup>

---

<sup>1102</sup> Morton Horwitz claims that common carriers faced strict liability for loss or injury to goods in their possession, other than those caused by "the act of god or the public enemies," until approximately 1830. Thereafter, the extent to which common carriers could limit their liability by "express contract" or by "notice" became one of the most vexed and inconclusive controversies of the century. See HORWITZ, *supra* note 193, at 204-07.

<sup>1103</sup> See Section V.A.2. (Secondary Roles of FCA), *supra*. For authoritative articulation of the definitional scope of "common carrier" in the telecommunications field, see *F.C.C. v. Midwest Video Corp.*, 440 U.S. 689, 700-01 (1979); *National Ass'n of Regulatory Util. Comm'rs v. F.C.C.*, 525 F.2d 630, 640-42 (D.C. Cir.), *cert. denied*, 425 U.S. 992 (1976). The FCC was established pursuant to the Communications Act of 1934, as amended (the "Act"), codified at 47 U.S.C. §§ 151 *et seq.* FCC regulations issued pursuant to the Act appear in Title 47 of the Code of Federal Regulations.

<sup>1104</sup> Loss of, or damage to, goods by an intermediary, setting aside questions of consequential damages, gives rise to monetary loss measured by their value or diminution in value. The same is *not* true of electronic (or other) communications because damages, again setting aside questions of consequential damages which may arise upon non-receipt or delay, are negligible.



## 1. Regulation of United States Telecommunications

Regulation is frequently used to limit the activities, revenues and liability of regulated entities.<sup>1105</sup> The FCC, state regulatory bodies<sup>1106</sup> and the so-called Modification of Final Judgment ("MFJ")<sup>1107</sup> in the AT&T antitrust litigation constitute a regulatory scheme<sup>1108</sup> which permits telecommunications service providers to enjoy the benefits of limited liability.

A telecommunications service provider must perform a regulated service to benefit from liability restrictions. The FCC regulates *common carriers* pursuant to Title II of the Act,<sup>1109</sup> which mandates the filing of tariffs setting forth, *inter alia*, services, rates and liability limitations.<sup>1110</sup> Tariffs must be "just and reasonable"<sup>1111</sup> and no carrier may engage in "unjust or unreasonable

---

<sup>1105</sup> "The Federal Communications Commission is now floating the idea of making carriers, rather than their customers, liable for losses due to fraudulent use of phone service . . . thereby shifting the weight of fraud prevention to carriers and equipment vendors. . . ." E. Messmer, *FCC getting tough on toll fraud*, NETWORK WORLD, Dec. 13, 1993 at 21. The FCC is [also] considering a Truth in Lending Act approach, *e.g.*, limiting liability to \$50.00. *Id.* Cf. 42 U.S.C. § 2010(e)(1) (imposing liability caps for nuclear power plant licensees), discussed at Section IX.B.3., *infra*.

<sup>1106</sup> State telecommunications regulation is beyond the scope of this paper. This paper assumes (perhaps too readily) that any FCA regulation will preempt state regulation. Cf. *California v. F.C.C.*, 905 F.2d 1217 (9th Cir. 1990) (reversing attempted preemption under 47 U.S.C. § 152(b)(1), which limits FCC jurisdiction over "intrastate" communications services).

<sup>1107</sup> *United States v. AT&T Co.*, 552 F. Supp. 131 (D.D.C. 1982) (subsequent history omitted).

<sup>1108</sup> See SAPRANOV, A PRIMER ON TELECOMMUNICATIONS LAW AND REGULATION, reprinted in TELECOMMUNICATIONS AND THE LAW 1 (W. Sapranov ed., 1988).

<sup>1109</sup> 47 U.S.C. §§ 201-228. "Common carrier" is defined to mean "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy. . . ." *id.* § 153(h).

<sup>1110</sup> See *id.* § 203.

<sup>1111</sup> *Id.* § 201(b).

discrimination."<sup>1112</sup> Tariffed liability limitations have been regularly enforced by the courts.<sup>1113</sup>

---

<sup>1112</sup> *Id.* § 202(a).

<sup>1113</sup> See, e.g., *Schaafs v. Western Union Tel. Co.*, 215 F. Supp. 419 (E.D. Wis. 1963); *Komatz Constr. Co. v. Western Union Tel. Co.*, 290 Minn. 129, 186 N.W.2d 691 (Min.), *cert. denied*, 404 U.S. 856 (1971); *Housing Auth. v. Western Union Tel. Co.*, 183 S.E.2d 227 (Ga.), *aff'd.*, 186 S.E.2d 100 (1971). The relevant language in *Komatz* was as follows:

ALL MESSAGES TAKEN BY THIS COMPANY ARE SUBJECT TO THE FOLLOWING TERMS:

To guard against mistakes or delays, the sender of a message should order it repeated, that is, telegraphed back to the originating office for comparison. For this, one-half the unrepeated message rate is charged in addition. Unless otherwise indicated on its face, this is an unrepeated message and paid for as such, in consideration whereof it is agreed between the sender of the message and the Telegraph Company as follows:

1. The Telegraph Company shall not be liable for mistakes or delays in the transmission or delivery, or for nondelivery, of any message received for transmission at the unrepeated message rate beyond the sum of five hundred dollars; nor for mistakes or delays in the transmission or delivery, or for nondelivery, of any message received for transmission at the repeated message rate beyond the sum of five thousand dollars, unless specially valued; nor in any case for delays arising from unavoidable interruption in the working of its lines.

2. In the event the Telegraph Company shall not be liable for damages for mistakes or delays in the transmission or delivery, or for the non-delivery, of any message, whether caused by the negligence of its servants or otherwise, beyond the actual loss, not exceeding in any event the sum of five thousand dollars, at which amount the sender of each message represents that the message is valued, unless a greater value is stated in writing by the sender thereof at the time the message is tendered for transmission, and unless the repeated message rate is paid or agreed to be paid and an additional charge equal to one-tenth of one percent of the amount by which such valuation shall exceed five thousand dollars.

186 N.W.2d at 693.



The FCC has decided not, however, to regulate so-called "enhanced service" activities. "Enhanced services" combine "basic" (pure transmission) services with "computer processing applications that act on the format, content, code, protocol or similar aspects of the subscriber's transmitted information; or provide the subscriber additional, different, or restructured information or involve subscriber interaction with sorted information."<sup>1114</sup> However, because these services use the transmission facilities of common carriers, the FCC regulates the interaction between the two classes of services to avoid (i) discriminatory access practices by basic service operators in favor of their affiliates; and (ii) use of regulated "monopoly" profits to subsidize enhanced services.

After almost three decades of mandating the use of separate subsidiaries for the provision of enhanced services,<sup>1115</sup> the FCC has relatively recently shifted course to permit both basic *and* enhanced services to be provided by the same corporate entity, subject to certain "nonstructural safeguards."<sup>1116</sup> These include special cost allocation methods and antidiscrimination provisions to ensure equality of access for non-basic service provider competitors.<sup>1117</sup>

---

<sup>1114</sup> 47 C.F.R. § 64.702(a); *see also In re Amendment of Section 64.702 of the Commission's Rules and Regulations*, 77 F.C.C.2d 384 (1980) [hereinafter *Computer II*], *on recon.*, 84 F.C.C.2d 50 (1980), *on further recon.*, 88 F.C.C.2d 512 (1981), *aff'd sub nom. Computer Communications Indus. Ass'n v. F.C.C.*, 693 F.2d 198 (D.C. Cir. 1982), *cert. denied*, 461 U.S. 938 (1983).

<sup>1115</sup> *See especially Computer II, supra* note 1114.

<sup>1116</sup> *See In re Amendment of Sections 64.702 of the Commission's Rules and Regulations*, 104 F.C.C.2d 958 (1986) [hereinafter *Computer III*], *on recon.*, 2 F.C.C. Rcd 3035 (1987); 2 F.C.C. Rcd 3072 (1987), *on further recon.*, 3 F.C.C. Rcd 1135 (1988); 3 F.C.C. Rcd 1150 (1988), *on second further recon.*, 4 F.C.C. Rcd 5927 (1989), *vacated sub nom. California v. F.C.C.*, 905 F.2d 1217 (9th Cir. 1990).

<sup>1117</sup> *See California v. F.C.C.*, 905 F.2d at 1229. The FCC's anti-discrimination initiative included provisions mandating certain notices and disclosures to competitors respecting service parameters and customer preferences. *See id.* at 1230. It also implemented an "open-network policy" consisting of "Comparably Efficient Interconnection" ("CEI") rights for competitors and, in the longer term, "Open Network Architecture" ("ONA"), which is intended to apply CEI principles to the "overall design of . . . basic service network[s]." *Id.* at 1233. The notion of ONA is poised to become one of the more profound philosophical issues in the "information superhighway" implementation. *See, e.g.,* Kapor, *supra* note 33.

The policies embodied in *Computer III* appear to be of considerable importance to the FCC. It responded to the Ninth Circuit's opinion vacating *Computer III* as "arbitrary and capricious"<sup>1118</sup> by reinstating a similar regime including "a strengthened set of nonstructural safeguards."<sup>1119</sup> This action is reportedly on appeal.<sup>1120</sup>

Assuming that FCA services meet the definition for "enhanced services" by acting on the "format . . . code, protocol or similar aspects of the subscriber's transmitted information," FCA services would probably not be regarded as tariffed ones and so regulated under that scheme. This is not to say that the FCC's current basic/enhanced classification scheme is immune to change, however. FCA services might represent a sufficiently novel form or facet of communication, linking commercial interests in the same way the telephone system originally linked individuals, that CAs might be deemed a new form of common carrier.

Even barring such formal reclassification, the FCA could also be classified as a common carrier if its services were considered "incidental to carriage."<sup>1121</sup> In response, however, the argument would be available that the FCA's principal purpose is to provide value-added services in the form of a more secure electronic environment.

It is conceivable that the FCA might attempt self-classification as a common carrier for the purpose of controlling liability. Another option is for the FCA to define part of its function as a common carrier and part as a provider of enhanced services. Because the FCC regulates the interaction between basic and enhanced services, the FCA might merit regulation, and liability protection, in this fashion.

---

<sup>1118</sup> *California v. F.C.C.*, 905 F.2d 1217.

<sup>1119</sup> *In re "Computer III" Remand Proceedings: Bell Operating Co. Safeguards and Tier I Local Exchange Co. Safeguards* (¶ 5), 6 F.C.C. Rec. 7571, (1991).

<sup>1120</sup> See Baker, *Legal Developments in Domestic Telecommunications and Information Services*, 33 JURIMETRICS J. 427, 437 & n.39 (1993).

<sup>1121</sup> 47 C.F.R. § 64.702(b), (c); cf. *In re North Am. Telecommunications Ass'n*, 101 F.C.C.2d 349 (1985) (designating many "CENTREX" services as "basic" under *Computer II*); 3 F.C.C. Rcd. 4385 (1988) (same result under *Computer III*).



## Impact of "Open Network Architecture" on the FCA

Bearing on the common carrier issues discussed above is the question of the FCA's position in the FCC's "Open Network Architecture" ("ONA") policy initiative. It would appear that the greater the FCA's integration into such an infrastructure, the more it would resemble a common carrier, albeit of a specialized type of communication. The FCA's role in the infrastructure could be that of a connection point. A "connection point" has been defined as "any installation or group of installations making possible the transmission, or the transmission and routing of telecommunications signals, and the exchange of the associated control and management information between the termination points in that network."<sup>1122</sup>

The exact impact of such status on the common carrier question is not clear. If the entire system were conceived of as an information highway, the FCA would appear to serve as guardian for certain access points and interchanges as if it operated a series of toll booths. The "highway" may be, operated by one or more common carriers, but whether access regulation is a separate common carrier service is a different question. A related way of examining the issue is to consider the degree to which FCA services would be "open" or "reserved." The more "open" the FCA is, the more likely it will resemble a common carrier.

Analogous to the FCC's ONA policy initiative is the European Community's "Open Network Provision" ("ONP") directive. Interestingly, this directive makes the following important distinction in terms of the requirement of "openness":

Open network provision conditions must not restrict access to public telecommunications networks or public telecommunications services, except for reasons based on essential requirements, within the framework of Community Law, namely:

- security of network operations,
- maintenance of network integrity,
- interoperability of services, in justified cases,
- protection of data, as appropriate . . . .<sup>1123</sup>

Pursuant to the foregoing, it is precisely in the area in which an FCA would operate -- telecommunications security -- that exceptions to openness may be

---

<sup>1122</sup> "Termination points" have been defined as "all physical connections and their technical access specifications which form part of the public telecommunications network and are necessary for access to and efficient communication through the public network."

<sup>1123</sup> Council Directive of 28 June 1990 on the Establishment of the Internal Market for Telecommunications Services Through the Implementation of Open Network Provision (90/387/EEC, OJ L 192/1, 24.07.90).

made. The FCA would be "open" to the extent that anyone could apply for a certificate, but "closed" to the extent that certificates may be denied or revoked. Screening an open network for security reasons would appear to be permissible under the ONP directive, yet it is difficult to decide or determine whether the "screener" itself would form a part of the network, standing, as it does, as a sort of barrier. It seems reasonable to assume that even gatekeepers are an important corollary to "openness," and therefore that the FCA might be considered as part of an open system: a status that would tend to militate in favor of common carrier status. Still another factor mitigating against the common carrier designation is the fact that the FCA could be considered "active" rather than "passive," in that it accepts and evaluates applications. Passivity is generally more in keeping with the role of a common carrier.

As this discussion indicates, a definitive answer to the common carrier question is difficult to reach, in part, because of the rapidly evolving notion of network architecture and services, as embodied in the FCA. This Report has merely attempted to set forth certain of the parameters affecting such a determination. An effective, but cumbersome, means of limiting FCA liability might be to designate it as a common carrier, using aspects of the preceding analysis.

Another approach to this situation is that recommended by Brian Fontes, Chief of Staff for the FCC, which would involve a mixture of contracts and broad government limits on liability:

The fundamental issue facing deregulated telecommunication markets is the role, if any, of public policy/regulatory policy in formulating liability responsibilities. As telecommunications services become privatized, liability responsibilities should be negotiated between/among carriers, service providers and end-users. . . . [P]ublic policy should limit carriers to direct losses and carriers should not be liable for consequential losses, since telecommunication equipment and services are likely to differ in a competitive telecommunication marketplace, the issue of liability should be negotiated by contract<sup>1124</sup> between/among the affected parties. If carefully crafted, then both approaches could co-exist. Government broadly limits liability claims to direct losses, while individual contracts specify responsibilities and liabilities.<sup>1125</sup>

If an appropriate definition of "carriers" were used, the FCA might well fall under the scope of the policy. This approach warrants serious consideration.

---

<sup>1124</sup> Cf. *Simmons v. Columbus Venetian Stevens Bldgs., Inc.*, 155 N.E.2d 372 (Ill. App. 1958) (designating five types of relationships where public policy precludes limitation of liability for negligence: common carrier, innkeeper, bailor-bailee, employer-employee and landlord-tenant).

<sup>1125</sup> B. Fontes, *Rapporteur's Summary: Workshop on Liability and Interoperability Issues* (paper presented at the Sixth World Telecommunications Forum, Geneva, 1991).



## 2. Regulatory Regimes Abroad

### a. Recognized Private Operating Agencies

Just as the tariff system administered by the FCC has limited the liability of common carriers, foreign governments and transnational organizations have also placed limitations of liability on specific telecommunications services.<sup>1126</sup>

---

<sup>1126</sup> The following list provides citations to various national telecommunication liability laws and, in some cases, a few notes on the nature of those laws.

Belgium: The old Régie des Télégraphes adt Téléphones (RTT) is now defunct. Currently, under RTT's successor, Belgacom, liability is defined by Article 64 of the Law of 21 March 1991. *See* Moniteur Belge, 27 March 1991.

France: limitations on liability are in Article L.37 of the Post and Telecommunications Code.

Germany: the Deutsche Bundespost Telekom. Grundgesetz limits liability pursuant to sections 445-448 of the Telekommunikationordnung ("T.K.O.") and section 18, subsection 1.24, of the Ausland. T.K.O. (for international links). On July 1, 1991, the 1990 reform Art. 65 30 Postverf. replaced the T.K.O., indicating a growing preference for privately administered regimes.

Italy: Each telecommunication service has its own regulations, implementing the general principles set out in the Italian Postal Code. *See* Article 6 thereof.

Netherlands: Article 12 of the General Law (Wet op de telecommunicatievoorzienigen, Stb. 1988, 520) stipulates that there be no liability except upon malfunction or non-functioning of the telecommunications infrastructure. It allows damages for death or physical injury.

United Kingdom: Under Article 32 of the Telecommunications Act, organizations must ensure "reasonable skill and care." British Telecom limits liability to £50,000 per incident with a maximum of £1,000,000 for service mishaps, other than for physical injury. *See* Section 32 of 1982 Supply of Goods and Services Act. The Department of Trade and Industry defines value-added services. In April of 1990, liability was raised.

International telecommunications regulations are promulgated pursuant to the International Telecommunications Convention. The regulations are generally negotiated and formalized at World Administrative Telegraphic and Telephone Conferences. The International Telecommunications Union ("ITU") regulations for international interconnections apply to "Recognized Private Operating Agencies" ("RPOAs"), which have been defined as:

private operating agenc[ies] which operate[] a public correspondence or broadcasting service, and upon which the obligations provided for in Article 44 of the Convention are imposed by the Member in whose territory the head office of the agency is situated, or by the Member which has authorized this operating agency to establish and operate a telecommunications service on its territory.<sup>1127</sup>

RPOA status confers an official imprimatur of recognition and approval on the subject entity.<sup>1128</sup> The FCC views RPOAs as "transport services" rather than data processing/basic access capability services. Accordingly, most International Value Added Networks (IVANs) and EDI providers are not eligible for RPOA status. Under this sort of analysis, it seems more likely for the FCA to be considered a

---

*See generally* Spaeth, Comment, *A Comparative Study of the Regulatory Treatment of Enhanced Services in the U.S. and European Community*, 9 N.W.J. INT'L. L. & BUS. 415, 425-26 (1988).

For a discussion of the possible contours of the liability landscape in the European Communities, *see* Comm'n of the Eur. Community, *Towards a Dynamic European Economy: Green Paper on the Development of the Common Market for Telecommunications Services and Equipment* (Comm. No. 290; June 30, 1987); Council Decision Concerning the Establishment of a Plan of Action for Setting Up an Information Services Market, OJ No. L 288, 21. 10. 1988 at 39 (88/524/EEC); Report of the Working Group of Telecommunications, Information Technology and Broadcasting to the ABA Special Task Force on EC 1992 and The Council of the European Commission, Common Position Adopted by the Council of Feb. 5, 1990 With a View To Adopting A Directive on the Establishment of the Internal Market for Telecommunications Services Through Implementation of Open Network Provision, Council Directive No. 4078/90.

<sup>1127</sup> ITU Plenipotentiary Convention, Nairobi, at 149. The so-called "Nairobi Convention" is due to be superseded by the Nice Convention of 1989.

<sup>1128</sup> *See, e.g.*, RPOA Order, 104 F.C.C. 2d 214, 215 n.21 (1986).



"base access capability service" rather than a "transport service," and thus probably not considered an RPOA.<sup>1129</sup>

### 3. Operators of Transport Intermediaries in International Trade

There are major legal and practical differences among transportation and computer-based communications infrastructures that make highly tenuous any proposal to harmonize or adopt the former's legal regime into the developing rules of the latter. The difficulty in harmonizing the two results from the essential legal character of transport instruments being fundamentally linked to assurances of their need to be identified either as originals or copies. Identification in turn, is tied for reasons of simplicity, trust and custom to "tangible" paper-based manifestations. Other differences include that:

- (i) shipping is a physical undertaking unlike computer-based communications in many important respects;
- (ii) shipping (and in particular maritime shipping) has historically involved greater risks than other transportation or communication mechanisms<sup>1130</sup>;
- (iii) the goods shipped have intrinsic value as compared to computer-based communications which can be copied an infinite number of times and retained indefinitely at little relative expense; and
- (iv) shipping, in the case of maritime law, has certain rules, *e.g.*, "in rem liability of vessel" or the "general average," that are without close

---

<sup>1129</sup> These regulatory issues may have bearing on the designation of one or more public key infrastructure "root authorities" gaining international status. See Report by the Secretary General, ITU, *Participation of Entities and Organizations Other than Administrations in the Activities of the Union*, Doc. C93/49-E (3 June 1993) (contains a recommendation for the Council "to consider the recommended criteria and procedures for admitting new categories of "members" as well as recommendations related to the "rights and obligations" necessary to ensure effective participation of these "members").

<sup>1130</sup> For example, historically, a sailing ship could be out to sea for months without any communication to port; weather and pirates posed tremendous risks. In contrast, computer-based communications are either nearly instantaneous or of comparatively short duration. Even with the expedited movement of cargo, shipping is still not instantaneous, and, in addition, is physical, thereby adding to the risk of loss or danger.

analog in computer-based communications law or commercial practices.

However, due to the significant historical value of liability analysis in transportation, and in particular shipping law, this section is included.<sup>1131</sup> Also, the provisions of transportation law respecting consequential damages are particularly interesting to contrast with those of communications law.

The first liability scheme for transportation intermediaries to be considered is that of operators of international transport terminals. The United Nations Convention on the Liability of Operators of Transport Terminals in International Trade (the "Liability Convention")<sup>1132</sup> was developed "to facilitate the movement

---

<sup>1131</sup> At the outset of this discussion, the author notes that respected members of the admiralty bar do not recognize a viable relationship, or even relevance, between maritime principles and telecommunications carriers and information security legal issues. Despite such assertions, transport documentation law issues increasingly contemplate the use of computer-based media and trusted intermediaries. *See generally Measures to Facilitate Maritime Transport Documents Procedures*, Recom. 12/Rev.1, UN/ECE/TRADE/WP.4/190 (July, 1993) [hereinafter Recommendation 12]. As noted below, the complex and diverse liability attributes of transport law are pedagogically rich.

However, "the links among the following schemes are interesting in terms of how they facilitate the *entire* transaction. Each component has a feature unique to it and some interface to the others. In this sense, there is an analogy to communication. This is true as well in terms of the relationship between the system of liability and other means of spreading risk, such as insurance. Although there are striking differences based on differing needs and structures, the great common factor is their resemblance in addressing these issues." Letter from Prof. James Byrne to Michael Baum (Apr. 18, 1994) (on file at Independent Monitoring).

<sup>1132</sup> Done at Vienna, April 19, 1991 (not yet in force), *reprinted in* UNCITRAL: The United Nations Commission on International Trade Law, Annex VI, at 195 (2d ed., adv. version, 1992). *See also* Sweeney, *New U.N. Convention on Liability of Terminal Operators in International Trade*, 14 *FORDHAM INT'L L.J.* 1115 (1991).

"Operator of a transport terminal" is defined as:

a person, who, in the course of his business, undertakes to take in charge goods involved in international carriage in order to perform or to procure the performance of transport-related services with respect to the goods in an area under his control or in respect of which he has a right of access or use. However, a person is not considered an operator whenever he is a carrier under applicable rules of law governing carriage.



of goods by establishing uniform rules concerning liability for loss of, damage to or delay in handing over such goods while they are in the charge of operators of transport terminals and are not covered by the laws of carriage arising out of conventions applicable to the various modes of transport."<sup>1133</sup> Under the Liability Convention, the operator is liable for losses that result when goods are lost, damaged, or delayed while under the operator's control, unless the operator can prove that he "took all measures that could reasonably be required to avoid the occurrence and its consequences."<sup>1134</sup> However, "the operator is liable only to the extent that the loss is attributable to [his] failure, provided that the operator proves the amount of the loss not attributable thereto."<sup>1135</sup>

"When the loss of or damage to a part of the goods affects the value of another part of the goods," the extent of the damage will be taken into consideration in determining the limit of liability.<sup>1136</sup> "Liability for delay in handing over the goods . . . is limited to an amount equivalent to two and a half times the charges

---

Liability Convention art. 1, § (a). "Terminal" does not imply *transport*, but is an essential adjunct of the continuation of the process "[w]here goods are consolidated in a container, pallet or similar article of transport where they are packed, 'goods' includes such article of transport or packaging if it was not supplied by the operator." *Id.* art. 1, § (b).

<sup>1133</sup> *Id.* Preamble.

<sup>1134</sup> *Id.* art. 5, § 1.

<sup>1135</sup> *Id.* art. 5, § 2. Loss is limited to an amount not exceeding 8.33 "units of account" per kilogram of gross weight of the goods lost or damaged, except when the goods are handed over to the operator immediately after carriage by sea or by inland waterways, in which case liability is limited to 2.75 units of account per kilogram. *Id.* art. 6, § 1(b).

A *unit of account* is defined as an International Monetary Fund Special Drawing Right (SDR), *see id.* art. 16, § 1, which in turn is a weighted basket of currencies worth \$1.4219 (as of Oct. 13, 1993). The criteria that are to be used in determining the propriety and measurement of future amendments to the limitation amounts include: amounts by which limits have been amended in any transport-related conventions, the value of goods handled by operators, the cost of transport-related services, insurance rates, average level of damages awarded against operators for loss or damage to, or delay in handing over, goods and the cost of electricity, fuel and other utilities. *See id.* art. 24, § 4.

<sup>1136</sup> *Id.* art. 6, § 1(c).

payable to the operator for his services in respect of the goods delayed, but not exceeding the total of such charges in respect of the consignment of which the goods were a part."<sup>1137</sup> These liability limitations are applicable to actions, whether founded in contract or tort,<sup>1138</sup> but are not applicable when damages occur as a result of intentional or reckless action on the part of the operator "with the knowledge that such loss, damage or delay would probably result."<sup>1139</sup>

The Liability Convention includes special rules on dangerous goods which exonerate the carrier if such goods "are handed over to the operator without being marked, labeled, packaged or documented . . . ." <sup>1140</sup> If the operator participated in a survey or inspection of the goods at the time when they were delivered to the person so entitled, notice need not be given of loss or damage ascertained at that time.<sup>1141</sup> "No compensation is payable for loss resulting from delay in handing over the goods unless notice has been given to the operator within 21 consecutive days after the day when the goods were handed over to the person entitled to take delivery of them."<sup>1142</sup> Article 12 establishes limitations periods and includes a general limitations period of two years.<sup>1143</sup>

These rules are potentially relevant to the FCA to the extent it would function as, or can be characterized as, an *electronic transport terminal* of sorts.<sup>1144</sup> For

---

<sup>1137</sup> *Id.* art. 6, § 2.

<sup>1138</sup> *See id.* art. 1, § 1.

<sup>1139</sup> *Id.* art. 8, § 1.

<sup>1140</sup> *Id.* art. 9, § 1.

<sup>1141</sup> *See id.* art. 11, § 3.

<sup>1142</sup> *Id.* art. 11, § 5.

<sup>1143</sup> *See id.* art. 12, § 1.

<sup>1144</sup> To the extent that terminal operators serve as subcontractors to ocean carriers, their relevance to the FCA is probably diminished. However, if long-term storage is needed, terminal operators may contract directly with cargo owners. Also, terminal operators can be analogized to many of the third parties that participate in computer-based trading partner interconnection but who lack privity with both trading partners. A closer FCA analog may be the freight forwarder who performs value-added services for both sides of transactions.

One particular problem concerns determining what are the generally understood principles of accountability and in what situation the parties can "agree" to more



example, in an FCA environment, the FCA could provide assurances analogous to those provided by transport terminal operators as to the status or quality of a transaction or the message representing it.

#### 4. The Hague, Hamburg, and Other Rules

A different type of intermediary role is played by ships transporting goods overseas. A short history of the development of liability rules in this area appears below. The account is instructive for FCA purposes because it illustrates the historic struggle over liability limits between two historically competing interests: carriers and shippers (an FCA analog being the originator and intermediary of a communication):

Historically, maritime law held the carrier absolutely liable for loss of or damage to cargo, whether or not he was negligent and (with a few exceptions) regardless of the cause of loss. . . .

However, by the end of the last century ocean carriers had managed to limit their liability for the carriage of goods by sea to a degree that finally became unacceptable to cargo interests, i.e., shippers and consignees. In the United States this resulted, in 1893, in the so-called "Harter Act" [27 Stat. 445 (1893) (codified as amended at 46 U.S.C. App. §§ 190-96 (1988))] being passed. This act placed certain minimum but mandatory liabilities on the carriers in order to offer the merchants at least some protection.

This did not, however, end the controversy, and at the beginning of the second decade of this century, negotiations were held, resulting in a diplomatic conference [that produced] the International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading, commonly known as the Hague Rules.

The Hague Rules were welcomed by most shippers and consignees but had been adopted against the wishes of ship owners, who opposed the increase in their liabilities which the new Convention caused. One of the arguments used against the rules was that insurance premiums would increase owing to the increased carrier liability.<sup>1145</sup>

---

or less and to what extent the law will save them from their agreement. Letter from Prof. James Byrne,*supra* note 1131.

<sup>1145</sup> UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, THE ECONOMIC AND COMMERCIAL IMPLICATIONS OF THE ENTRY INTO FORCE OF THE HAMBURG RULES AND THE MULTIMODAL TRANSPORT CONVENTION, REPORT BY THE SECRETARIAT, AT 6 TD/B/C.4/315 (PART ONE) (31 Dec. 1987) [hereinafter UNCTAD REPORT]. The Hague rules are formally entitled the International Convention for the Unification of Certain Rules Relating to Bills of Lading (1924). See E. Caprioli, *EDI et droit du commerce international: état de l'environnement légal*, Lamy droit de l'informatique, Supp. au N° 43, at 12-14 (Dec. 1992) (surveying the status of various international transport conventions and treaties).

However, as noted by Professor Kozolchyk:

The Hague Rules, COGSA [Carriage of Goods by Sea Act], and the Harter Act regarded the sea voyage itself as a risk sharing venture between shippers and carriers. Since the carriers risked their ships, it was assumed that they would select and supervise their crews with enough care to prevent the damages that could result from improper management and navigation of the ship. Such damages were therefore exempted by the Hague Rules, as were those caused by fire (unless caused by the design or neglect of the carrier), and by traditionally exempt perils, acts and events.<sup>1146</sup>

The Hague Rules were subsequently amended by the Visby Protocol in 1968<sup>1147</sup> to accommodate the realities of containerization and other technological developments. The rules became known as the Hague-Visby Rules. The United Nations Commission on International Trade Law ("UNCITRAL") subsequently undertook its own review of cargo liability rules and adopted the Hamburg Rules in 1978.<sup>1148</sup>

Recognizing the reduction of risks associated with maritime transport, the Hamburg Rules are intended to "strike a fairer balance in the allocation of risks, rights and obligations in the rules on liability between carriers and shippers."<sup>1149</sup> The Rules are modeled on conventions relating to land and air carriage, "particularly the Convention on the Contract for International Carriage of Goods by Road (CMR) and the Warsaw Convention,<sup>1150</sup> both of which have passed the test of practical applicability," (at least from UNCITRAL's viewpoint) as well as the Liability Convention, which in terms of liability provisions they closely resemble. This generally means that "the burden of proof rests on the carrier" to establish the absence of fault, although "with respect to certain cases, the provisions of the Convention modify this rule."<sup>1151</sup> The Hamburg Rules

---

<sup>1146</sup> Kozolchyk, *supra* note 26, at 188.

<sup>1147</sup> PROTOCOL TO AMEND THE BRUSSELS INTERNATIONAL CONVENTION OF 25 AUGUST 1924 FOR THE UNIFICATION OF CERTAIN RULES OF LAW RELATING TO BILLS OF LADING (Feb. 23, 1968).

<sup>1148</sup> Done at Hamburg, Mar. 31, 1978; entered into force on Nov. 1, 1992 [hereinafter HAMBURG RULES].

<sup>1149</sup> UNCTAD REPORT, *supra* note 1145, ¶ 99, at 4.

<sup>1150</sup> 49 U.S.C. App. § 1502 note. See Larson, 1989 *Inter-American Convention on International Carriage of Goods by Road*, 1 AM. J. COMP. L. 121 *et seq.* (1991).

<sup>1151</sup> HAMBURG RULES, *supra* note 1148, art. 5.1. Moreover, the carrier cannot rely on the nautical faults defense, which had been included in Rule 2(a) of the Hague



recognize the importance of the freight forwarder and other intermediaries and in this regard adopt an "end-to-end" rather than the "tackle to tackle" (point-to-point) approach taken in the Hague Rules.<sup>1152</sup> This change in scope independently parallels the trend toward the use of multiple TPSPs and intermediaries for computer-based communications that utilize end-to-end information security architectures.

The limits on liability currently codified in the Hamburg Rules are not significantly inconsistent with those of the Liability Convention. For example, the shipper must indemnify the carrier against losses relating to the "accuracy of particulars relating to the general nature of the goods" because of the fact that ships can be fined by customs for failing to correctly describe such goods.<sup>1153</sup>

---

Rules. The *nautical faults* defense under the Hague Rules relieved carriers of responsibility for "loss or damage arising or resulting from act, neglect, or default of master, mariner, pilot or the servants of the carrier in the navigation or the management of the ship." UNCTAD REPORT, *supra* note 1145, at 17. It should be noted that there is a worldwide trend toward imposing greater liabilities for carrier-related losses whether or not the nautical faults defense is available. *Id.* The UNCTAD REPORT states, "[s]ome shipowners are now ready to accept the abolition of the nautical faults defense and simultaneously agree to an increase in the limits of liability even exceeding those of the Hamburg Rules." *Id.* at 4. However, some recognized maritime experts vigorously assert the contrary. Interview with George F. Chandler, Esq., in Vienna (Oct. 11, 1993).

<sup>1152</sup> See Kozolchyk, *supra* note 26, at 196.

<sup>1153</sup> The relevant article states in full:

The shipper is deemed to have guaranteed to the carrier the accuracy of particulars relating to the general nature of the goods, their marks, number, weight and quantity as furnished by him for insertion in the bill of lading. The shipper must indemnify the carrier against the loss resulting from inaccuracies in such particulars. The shipper remains liable even if the bill of lading has been transferred by him. The right of the carrier to such indemnity in no way limits his liability under the contract of carriage by sea to any person other than the shipper.

HAMBURG RULES, *supra* note 1148. Art. 17.1. Art. 17.2 continues:

Any letter of guarantee or agreement by which the shipper undertakes to indemnify the carrier against loss resulting from the issuance of a bill of lading by the carrier, or by a person acting on his behalf, without entering a reservation relating to particulars furnished by the shipper for insertion in the bill of lading, or to the apparent condition of the

Certain measures do not limit liability exposure *per se*, but focus on reducing the cost of litigation by promoting arbitration and validating certain choice of law and choice of forum clauses in contracts.<sup>1154</sup> Supplementary provisions include those which authorize stipulations deviating from the Hamburg Rules and "assigning benefit of insurance of goods in favour of the carrier."<sup>1155</sup>

According to the UNCTAD Report, the overall effect of the Hamburg Rules will be to "shift liability from cargo owner to carrier and in this way better protect shippers the world over. However, it is a mild shift. . . ."<sup>1156</sup> Critics of the Hamburg Rules, including the (U.S.) Maritime Law Association, contend that the shift in liability is at odds with commercial reality.<sup>1157</sup>

---

goods, is void and of no effect as against any third party, including a consignee, to whom the bill of lading has been transferred.

*Id.* Art. 17.2.

<sup>1154</sup> See UNCTAD REPORT, *supra* note 1145, at 28.

<sup>1155</sup> HAMBURG RULES, *supra* note 1148, art. 23.

<sup>1156</sup> UNCTAD REPORT, *supra* note 1145, at 28.

<sup>1157</sup> See, e.g., Telephone Interview with George F. Chandler, Esq. (Aug. 2, 1993). Chandler notes that since 1978, 40 percent of the world has chosen Hague-Visby over the Hamburg Rules. A recent UN Regional Report advised countries to merely revise Hague-Visby rather than adopt the Hamburg Rules. Also, recent commentary on the Hague Rules and the Liability Convention "advised states already parties to the Hague Rules, so as to modernize the existing regime, to add to the regime based on the Hague Rules certain provisions based on the Hamburg Rules." Secretariat, Econ. and Commission for Asia and the Pacific, Guidelines for Marine Legislation (Guidelines Vol. 1, 3rd ed., ST/ESCAP/1076). This recommendation was proffered despite the U.N. General Assembly's resolution 47/34 of November 25, 1992 requesting the Secretary General to make increased efforts to promote wider adherence to the [Hague] convention." Report of the UNCITRAL on the work of its 26th sess., Jul. 5-23, 1993 (Gen. Assb'y Supp. No. 17 (A/48/17)) at ¶ 316.

There are other U.N. Conventions governing international carriage as well. See, e.g., Convention for the Unification of Certain Rules Relating to International Carriage by Air (12 October 1929) (the "Warsaw Convention"); United Nations Convention on International Multimodal Transport of Goods (Geneva, 1980). See generally Coffey, *Multimodalism and the American Carrier*, 64 TUL. L. REV. 569 (1989). Discussion of related topics may be found, e.g., in Griggs, *Coverage, Warranties, Concealment, Disclosure, Exclusions, Misrepresentations, and Bad*



## 5. Bills of Lading

A document commonly used to govern the rights of parties to goods transported by third parties, and of potential value as a model for developing part of the FCA infrastructure, is the bill of lading.<sup>1158</sup> A bill of lading is a cargo receipt, contract of carriage and a document of title. It is also sometimes defined as "a document evidencing the receipt of goods for shipment issued by a person engaged in the business of transporting or forwarding goods, and includes an airbill."<sup>1159</sup>

The bill of lading's *trust functionality* [including "reliable public notice"] also merits mention. Kozolchyk notes that "[s]hippers needed a document that could be issued by someone trustworthy in control . . . [i.e.] the ship's master . . . . In placing this responsibility on the master, European maritime law likened the master's duties of certification and giving notice to those of a quasi judicial official

---

*Faith*, 66 TUL. L. REV. 423 (1991); Letly, *Division of Collision Damages: Common Law, Civil Law, and Conflicts of Law*, 16 TUL. MAR. L.J. 263 (1992); Note, *Deviation and the Package Limitation in the Hague Rules and the Carriage of Goods By Sea Act: An Alternative Approach to the Interpretation of International Uniform Acts*, 68 TEX. L. REV. 977 (1990).

<sup>1158</sup> See Kozolchyk, *supra* note 26, at 161-245 (describing the historical development of, and suggesting the structure for, a bill of lading as a device to facilitate the computer-based certification of assurances required for international transactions). Another issue raised by Kozolchyk that is relevant to FCA policy statements (see section IX.C., *infra*) and liability is *privity of contract*. He notes that the English Bill of Lading Act of 1855 "filled the privity gap by allowing contractual rights against the carrier to be conveyed by possession of the bill of lading. Thereafter, statutory law became the main source for sanctioning documents of title." Kozolchyk, *supra*, at 170 & n.170.

<sup>1159</sup> "'Airbill' means a document serving for air transportation as a bill of lading does for marine or rail transportation, and includes an air consignment or air waybill." U.C.C. § 1-201(6). The Hamburg Rules define "bill of lading" as "a document which evidences a contract of carriage by sea and the taking over or loading of the goods by the carrier, and by which the carrier undertakes to deliver the goods against surrender of the document. A provision in the document that the goods are to be delivered to the order of a named person, or to order, or to bearer, constitutes such an undertaking." HAMBURG RULES, *supra* note 1148 art. 1(7).

referred to in the law of land based trade as a scrivener or notary public."<sup>1160</sup> Initiatives to accommodate computer-based negotiability of transport documents may demand such trust functionality.<sup>1161</sup>

---

<sup>1160</sup> Kozolchyk, *supra* note 26, at 168-69. Kozolchyk further references an article that describes the ship captain's role as similar to that of a notary public. *See* J. de Veitia, Norte de la Contratación de las Indias Occidentales 687 (1672, facsimile edition 1945). *See generally* Section VIII.D., *infra* (concerning notaries public). Prof. Byrne has queried whether ship's masters are uniformly "authorities" or whether their role is simply invoked by tradition. Letter from Prof. James Byrne, *supra* note 1131.

Kozolchyk also addresses "notice" requirements:

The first legal prerequisite involved in satisfying the transnational needs of the electronic bill of lading . . . is reliable public notice. Throughout the history of documents of title, possession provided reliable public notice of legitimacy of acquisition. Two reasons prevent it from continuing to provide this function. Possession of an electronic bill would be symbolic at best and, thus, would not be apparent to third parties and notice on items such as capacity or authenticity of issuance is not connected with possession of the bill or its electronic equivalent. Given the need for reliability, transactional neutrality and ease of access, a public type of bill of lading registry seems the logical choice.

Kozolchyk, *supra* note 26, at 243.

<sup>1161</sup> *See* ELECTRONIC CONTRACTING, *supra* note 2, ch. 11 (describing various initiatives to automate the bill of lading process); Recommendation 12, *supra* note 1131. The Interstate Commerce Commission has proposed regulations which state that "[a]ll common carriers, except express companies, engaged in the transportation of property other than livestock and wild animals, by rail or by water subject to the Interstate Commerce Act are required to use bills of lading . . . [to] be either documented on paper or generated and/or transmitted electronically." 58 Fed. Reg. 34,775, 34,776 (June 29, 1993) (proposing revision of 49 C.F.R. ch. X, part 1035).



## 6. Liability of "Warehousemen"<sup>1162</sup> for Title Information

When the FCA receives a public key certificate application containing certain information to be included in the certificate the situation is analogous (or at least instructive) to a warehouseman's receipt of documents of title containing information regarding goods. The questions that arise are to what extent is the intermediary liable for the accuracy of that information and what is the duty of the intermediary to check its accuracy.<sup>1163</sup> Section 7-203 of the Uniform Commercial Code indicates clearly that "non-receipt or misdescription" of the goods are generally not a basis for warehouseman liability:

A party to or purchaser for value in good faith of a document of title other than a bill of lading relying in either case upon the description therein of the goods may recover from the issuer damages caused by the non-receipt or misdescription of the goods, except to the extent that the document conspicuously indicates that the issuer does not know whether any part or all of the goods in fact were received or conform to the description, as where the description is in terms of marks or labels or kind, quality or condition, or the receipt or description is qualified by 'contents, condition and quality unknown', 'said to contain' or the like, if such indication be true, or the party or purchaser otherwise has notice.<sup>1164</sup>

The standard of care required to be exercised by a warehouseman is "such care in regard to [the goods] as a reasonably careful man would exercise under like circumstances but unless otherwise agreed he is not liable for damages which could not have been avoided by the exercise of such care."<sup>1165</sup> However, "[d]amages may be limited by a term in the warehouse receipt or storage

---

<sup>1162</sup> A *warehouseman* is "a person engaged in the business of storing goods for hire." U.C.C. § 7-102(h).

<sup>1163</sup> Various state and federal electronic registry initiatives merit consideration. These include U.C.C. Article 9 (Secured Transactions) registry filing systems, such as those in North Dakota and Louisiana. See ELECTRONIC CONTRACTING *supra* note 2, § 5.12 at 247-52; T. F. O'Malley & J. Olea, *A Comparison of U.S. and Mexican Warehouse Receipts Law and Practice*, in 1 TOWARDS SEAMLESS BOARDERS, MAKING FREE TRADE WORK IN THE AMERICANS 510-18 (B. Kozolchyk, ed. 1994). Also noteworthy is the development of rules to support registries for mobile equipment such as the UNCITRAL draft INTERNATIONAL CONVENTION GOVERNING THE RECOGNITION AND ENFORCEMENT OF SECURITY INTERESTS IN MOBILE EQUIPMENT. See T. Whalen, *The Proposed Convention Governing the Recognition and Enforcement of Security Interest in Mobile Equipment*, COMM. L. ANN. (forthcoming 1994).

<sup>1164</sup> U.C.C. § 7-203; *cf.* note 116, *supra* (contrasting the obligations for accuracy in applications for insurance and for a public key certificate).

<sup>1165</sup> *Id.* § 7-204(1).

agreement. . . . [but not] with respect to the warehouseman's liability for conversion to his own use."<sup>1166</sup> The law remains uncertain concerning the effect of contributory negligence on the part of the bailor.<sup>1167</sup> Finally, courts have permitted the recovery of lost profits for violation of the standard of care in section 7-204.<sup>1168</sup> The use of computer-based systems to facilitate the transfer of title via warehouse receipts presents certain challenges that the FCA may help to resolve.<sup>1169</sup>

---

<sup>1166</sup> U.C.C. § 7-204(2).

<sup>1167</sup> See *Fugate v. Brockway*, 937 F.2d 960 (4th Cir. 1991) (holding that violation of U.C.C. § 7-204 standard of reasonable care did not preclude bailor's recovery from a bailee). Section VIII.C.3., *supra* (concerning bailments).

<sup>1168</sup> See *Indemnity Marine Assurance Co. v. Lipin Robinson Warehouse Corp.*, 297 N.W.2d 846 (Mich. App. 1980); WHITE & SUMMERS, *supra* note 325, §§ 21-23.

<sup>1169</sup> On October 28, 1992, the United States Warehouse Act was amended, in part, to provide for the use of electronic cotton warehouse receipts. See 7 U.S.C. § 259(c). The amendment may lend further support to the legal efficacy of computer-based commerce by advancing the quest for computer-based negotiability. Since March of 1993, a corresponding draft regulation has been pending at the Office of the Management and Budget which may propose, in part, that electronic warehouse receipts systems providers (a form of computer-based intermediary) must carry typical computer insurance and maintain a certain level of net equity and bonding.

In a typical transaction, the buyer receives a receipt from the system provider representing cotton in a warehouse deliverable to the holder. Each receipt represents a certain amount of warehoused cotton. As with other agricultural commodities, it is possible for a third party to place a lien on the cotton. Accordingly, the buyer must check for the existence of liens. Upon redemption of the receipt with the system provider, the cotton is shipped to the buyer.

If a warehouse ships a bale without the receipt, the warehouse is liable. Under an electronic regime, if the electronic receipt is incorrect because of the system provider, then the warehouse should look to the system provider for redress.



## H. SECURITIES RULES

The following are several instances in which the Securities and Exchange Commission ("SEC") or other authority has proposed or promulgated liability rules regarding electronic filings or transactions. The SEC's general tendency has been to limit the liability of the system provider, and to place the brunt of the losses on exchange members. This suggests that an FCA, which would also handle a large number of financial transactions, might also be protected from liability in similar ways. Diverse securities rules, including relevant portions of U.C.C. Article 8 ("Investment Securities") and stock exchange clearing rules may further contribute to the development of certain viable FCA liability apportionment alternatives.

### 1. EDGAR

The SEC has implemented and mandated use of its Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") system and has issued rules applicable to various electronic submissions and notices thereunder. Mandated electronic filing for particular purposes and parties commenced April 26, 1993.<sup>1170</sup>

The EDGAR system has been "live" since July 1992 and currently receives submissions from approximately 3,400 entities. As EDGAR matures, that number

---

<sup>1170</sup> S.E.C., Rulemaking for EDGAR System, 58 Fed. Reg. 14,628 (Mar. 18, 1993) (amending existing rules and adopting new Regulation S-T which governs submission of electronic filings (17 C.F.R. Part 232)).

See note to Rule 13 of Regulation S-T: "Filers are strongly encouraged to submit the Form ID three to six months prior to becoming subject to mandated electronic filing in order to allow them the opportunity to become familiar with EDGAR procedures and prepare test filings." 58 Fed. Reg., at 14,633. The Form ID must be used to request passwords and CIK confirmation codes ("CCCs"), as well as a password modification authorization code ("PMAC"). In certain instances it must also be used to request central index key ("CIK") numbers. See Approval of FIPS PUB 181, Automated Password Generator (APG), 58 Fed. Reg. 51,802 (Oct. 5, 1993) (providing for an algorithm to "select the characters that form the random pronounceable passwords").

Furthermore, a June 1, 1995 federal deadline for computer-based trading of stocks and bonds raises further concerns, as exemplified by one brokerage firm. "[i]f the only proof of ownership [of securities] that you have is the statement from a brokerage firm,' investors will increasingly favor big-name financial supermarkets instead of the hundreds of regional brokerage firms." A. Peers, *'Paperless' Wall Street Is Due Next June*, N.Y. TIMES, June 7, 1994, at C1, C4.

should rise to approximately 15,000 entities. The EDGAR Link Software costs less than three dollars and includes compression capabilities. The EDGAR electronic filings use what the SEC characterizes as a *typed and electronically submitted signature* for authentication. Signature requirements can be satisfied by log-in procedures if transmitted with an intent to authenticate; two levels of access codes are provided. In short, the SEC asserts that "[t]he security controls in the EDGAR system for access and transmission should help guarantee the viability of a typed signature system."<sup>1171</sup>

Liability rules for "transmission errors or omissions in documents filed via EDGAR" provide a safe harbor for the filer when there is "an error or omission in an electronic filing resulting solely from electronic transmission errors beyond the control of the filer . . . [and] where the error or omission is corrected by the filing of an amendment in electronic format as soon as reasonably practicable after the electronic filer becomes aware of the error or omission."<sup>1172</sup>

## 2. Electronic Display Books

On April 20, 1993, the SEC issued a notice of proposed rule change<sup>1173</sup> to adopt a policy statement absolving the New York Stock Exchange (the "NYSE") from liability for damages sustained by American Stock Exchange ("Amex") members and member organizations using the electronic display book on the Amex trading floor.<sup>1174</sup> The Amex Constitution currently provides that it shall not be liable for damages incurred by a member firm from the use of Amex facilities (which includes the use of Amex's trading systems) except as Amex may otherwise provide. It is recognized that liability for the system's use is a risk not properly borne by Amex. In connection with the display book agreement, the NYSE is requiring that it also be protected from liability with regard to member firm use of the display book on the Amex floor.

## 3. BEACON

Another stock exchange system subject to new liability regulations is the BEACON system used on the Boston Stock Exchange ("BSE"). The BEACON

---

<sup>1171</sup> 58 Fed. Reg. 14,628, 14,645 (Mar. 18, 1993).

<sup>1172</sup> 17 C.F.R. § 232.103; 58 Fed. Reg. 14,628, 14,673 (Mar. 18, 1993).

<sup>1173</sup> Release No. 34.31805; File No. SR-Amex-92-46.

<sup>1174</sup> See 58 Fed. Reg. 21,327 (Apr. 20, 1993).



system comes into play when an exchange-listed stock is handled by a registered broker or an exchange member. The brokerage firm will route the order to the floor electronically, where it is processed by the BEACON system and sent to a specialist. The order is also keyed into the system off-floor. The BSE, through the BEACON system, provides the system's hardware and software. If the sender of the order keys in the wrong price or its link does not re-transmit the message, then the BSE, under a recent rule, does not accept responsibility. However, if the system accepts the order, then the BSE will validate that the order has been received by the specialist. The regulation establishes liability rules for this system, which insulate the BSE from liability:

Sec. 7. In accordance with Article IX, Section 10 of the Exchange Constitution, the Exchange shall not be liable for any loss sustained by a member or member organization resulting from the use of the BEACON System. Generally, a loss pertaining to an order that is entered through the BEACON System and which does not appear on the BEACON System's Member Firm Interface Safe-Store File will be absorbed by the entering member organization. A loss pertaining to an order that is entered through the BEACON System which was designed for a particular specialist's post and which does not appear on the BEACON Systems' Member Firm Interface Safe-Store File will generally be absorbed by the specialist.<sup>1175</sup>

---

<sup>1175</sup> 57 Fed. Reg. 21,141 (May 18, 1992).

<sup>1175A</sup> J. Tenenbaum, EIT, Press Release (Palo Alto, Apr. 12, 1994). Mosaic is a point-and-click graphical interface for accessing diverse Internet services. WWW is a general-purpose architecture for Internet-based information retrieval. CommerceNet use is subject to the following warranty and liability provisions:

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL THE COMMERCE NET CONSORTIUM BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS INFORMATION.

## I. COMMERCENET

CommerceNet is a secure mosaic-based "large-scale market trial of electronic commerce on the Internet" that is intended to "unleash the commercial potential of the Internet by enabling buyers and sellers to meet spontaneously and transact business." It purports to "establish[] a valid framework for companies to immediately begin large-scale commerce on the Internet." Undertaken by Enterprise Integration Technologies, CommerceNet will integrate public key cryptography into National Center for Supercomputing Applications' Mosaic clients and World Wide Web servers to "provide the foundation for a broad range of financial services, including the network equivalents of credit and debit cards, letters of credit and checks" that will enable "all users to safely transact day-to-day business involving even their most valuable information on the Internet." CommerceNet will also certify public keys on behalf of member companies, and will authorize third parties such as banks, public agencies, and industry consortia to issue keys.<sup>1175A</sup>

---

Descriptions of, or references to, products or publications within the CommerceNet Information Server does not imply endorsement of that product or publication. CommerceNet Consortium makes no warranty of any kind with respect to the subject matter included herein, the products listed herein, or the completeness or accuracy of this catalog. CommerceNet specifically disclaims all warranties, express, implied or otherwise, including without limitation, all warranties of merchantability and fitness for a particular purpose.

CommerceNet's Subscriber Agreement includes the following liability provision:

You agree that CommerceNet will not be responsible to you for any indirect, consequential, special or punitive damages or losses you may incur in connection with or any of the data or other material provided through or residing on , even if has been advised of the possibility of such damage or loss. In addition, you agree to defend and indemnify and hold harmless from and against any and all claims, proceedings, damages, injuries, liabilities, losses, costs and expenses (including reasonable attorneys' fees) relating to any acts by you or materials or information provided in connection with leading wholly or partially to claims against operators of or our service by other users, subscribers or third parties.



## IX. OTHER APPROACHES TO MITIGATE LIABILITY

### A. CERTIFICATION AND ACCREDITATION

Because deserved confidence and trust in the FCA is of vital importance, mechanisms to assure its accountability, consistency and quality are indispensable. Such mechanisms must be tailored to operate within one of three areas that fall within the FCA's jurisdiction: entities, professionals, and products and services. Certification and accreditation of these categories is one such mechanism. The complexity of the roles and relationships among these groups; the meaning, legal and practical implications, limitations and boundaries of their respective certifications and accreditations; and the vehicles through which such certifications and accreditations can and should be provided all require exploration. This section briefly surveys a number of important certification and accreditation issues.

*Certification and Accreditation* have many definitions<sup>1176</sup> but are defined here generally as the process of approval or recognition by a trusted body representing

---

<sup>1176</sup> For example, the National Computer Security Center (NCSC) states as follows:

[Accreditation]: A formal declaration by the DAA [Designated Approving Authority] that the AIS [Automated Information System] is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

[Certification]: The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

NCSC, *Glossary of Computer Security Terms* 4, 8 (NCSC-TG-004, Oct. 21, 1988); cf. Dept. of Commerce/NBS, *Guideline for Computer Security Certification and Accreditation*, FIPS PUB 102 (Sept. 27, 1983) at 13 (referencing definitions from FIPS 39); NCSC, *Introduction to Certification and Accreditation* 31-32 (NCSC-TG-029 Ver. 1, Jan. 1994) (defining accreditation and certification).

A Danish administrative order provides:

that the subject (entity, professional, product, or service, as applicable) of such certification and accreditation has satisfied recognized criteria, typically concerning quality, performance, ethics, experience, safety, education, or competence. The FCA could develop performance criteria and testing for such certification and accreditation. The federal government is experienced in similar activities, and is aware of their importance.<sup>1177</sup>

---

[Certification]: shall mean ascertainment and attestation as to

- (1) whether a specified product, service or services is in conformity with a given standard or other specification,
- (2) whether a company's quality system is in conformity with given standards or other specifications,
- (3) whether a person's qualifications are in conformity with given specified requirements.

Order on Accreditation of Companies, Inc., for Certification of Persons, Products and Systems, Translation 168, 19 March 1991, Danish Ministry of Industry, Nat'l Agency of Industrial Trade, File No. 1988-201/035-1.

Webster provides a more general definition:

[Accreditation]: To recognize or vouch for as conforming with a standard . . . to recognize (an educational institution) as maintaining standards that qualify the graduates for admission to higher or more specialized institutions or for professional practice.

[Certify; Certification]: To attest as being true or as represented or as meeting a standard . . . to guarantee (a personal check) as to signature and amount by so indicating on the face.

WEBSTER'S NEW COLLEGIATE DICTIONARY 8, 182-83 (1977).

See also ISO/IEC Guide 2 "General terms and their definitions concerning standardization and related activities." See generally, National Commission for Certifying Agencies, *Criteria For Approval of Certification Programs* (amended Feb. 1990).

<sup>1177</sup> "In government contracting, the acquisition authority must determine and specify those performance-related features that are desired to be under user or application process control and those desired to be under system operator control. The [parties] . . . may also wish to specify benchmarking criteria as evidence of satisfying performance requirements." NIST, FIPS PUB 146 at 12.



FCA policies or agreements could impute predetermined legal significance to successful completion of accreditation and certification testing. For instance, trade transactions executed over an accredited interoperable system could be presumed accurate and enforceable (or more accurate and enforceable than others), such that parties would be estopped from denying the authenticity or integrity of information sent from certified systems unless probative evidence demonstrated otherwise.<sup>1178</sup>

Additionally, the successful completion of testing could also evidence an implementation's *commercial reasonableness*. Policies or agreements that apportion liability for erroneous transactions could be based on such successful completion.<sup>1179</sup> It might also become a legal prerequisite for the purchase or maintenance of insurance coverage<sup>1180</sup> or for the communication of sensitive or higher-risk information.<sup>1181</sup>

The following figure illustrates the triad of groups participating in, or benefiting from, accreditation and certification.<sup>1182</sup> The purpose and potential relevance of each of these groups to the FCA is discussed below.

---

<sup>1178</sup> See LINKING SECURITY, *supra* note 2, § IV., at 59-67 (considering presumptions).

<sup>1179</sup> The apportionment of liability based upon the implementation of reasonable security procedures already has legal precedent. See Section VIII.A.2., *supra* (concerning U.C.C. Article 4A).

<sup>1180</sup> See Section IX.B., *infra* (considering insurance issues).

<sup>1181</sup> See Garfinkel, *supra* note 393, at 46 (interviewing Peter G. Neumann concerning licensing of programmers).

<sup>1182</sup> "A certifying agency responsible for attesting to the competency of practitioners has a responsibility to the individuals desiring certification, to the employers of those individuals, to those agencies that may reimburse it for the service and to the public." Nat'l Comm. for Certifying Agencies, *Criteria for Approval of Certification Programs* (amend. Feb. 5, 1990) at 1. See generally E. Hines, *Credentialing EDI Trusted Entities* (paper presented to the Notarization and Nonrepudiation Work Group, Information Security Committee, EDI and Information Technology Division, Section of Science and Technology, ABA) (Wash., D.C., July 1-2, 1993).

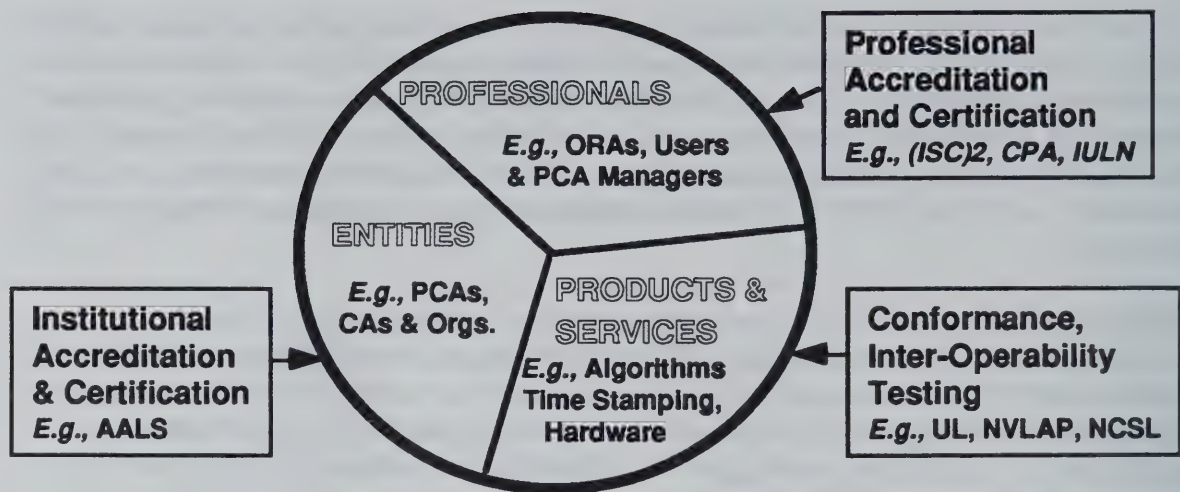


FIGURE 3 - INTEGRATION OF CERTIFICATION AND ACCREDITATION

Abbreviations Specific to Figure 3

AALS	American Association of Law Schools
CPA	Certified Public Accountant
(ISC) <sup>2</sup>	Information Systems Security Certification Consortium
IULN	International Union of Latin Notaries
NCSL	National Computer Security Laboratory
NVLAP	National Voluntary Laboratory Accreditation Program
UL	Underwriters Laboratories

## 1. Entities

Conventional "entity" examples include the accreditation of law schools as fulfilling the (quality) requirements of the American Bar Association, or of hospitals by the Joint Commission for the Accreditation of Healthcare Organizations. An obvious FCA-related example of entity-based accreditation and certification is the issuance of a public key certificate to a CA by its PCA *where the PCA's policy includes an entity review for conformance to the policy.*

Another aspect of entity accreditation and certification that might have an impact on the use of the FCA for business purposes concerns verification of the existence, solvency, location, and "good standing" of federal contractors or, perhaps later, private enterprises generally. For example, the issuance of public key certificates within the Chambers of Commerce's CEDI-FACT pilot<sup>1183</sup> might be developed to include an *implied* certification that the subject company was properly registered and in good standing with its local Chamber of Commerce. Other forms of

<sup>1183</sup> See Section VIII.E. ("Chambers of Commerce"), *supra*.



certification might include features analogous to Standard and Poor's bond ratings or ISO 9000 registration for quality management.

## 2. Professionals

In addition to entity certification and accreditation, the trustworthiness and quality of the *individuals* involved in operating the FCA, as well as in supporting institutions (e.g., super notaries<sup>1184</sup>), are important:

Pervasive throughout the free American society and economy is the concept of credentialing of professionals and institutions. Those who use professional services or follow academic programs seek and expect objective evaluation of the quality of those services or programs. Credentialing is often relied upon intuitively; users come to expect it and may be surprised when they find that it is absent. Traditionally, the quality criteria for certification and accreditation have been established and promulgated by private, nonprofit, voluntary organizations -- professional societies or educational associations, independent boards or councils, or other nongovernmental groups -- which also conduct evaluations of professionals or institutions to determine if the criteria are met. Credentialing serves an enormously valuable function. Most citizens are not equipped to determine whether minimum competency has been achieved by professionals or institutions.<sup>1185</sup>

The importance of accreditation of information security professionals has been expressed by the International Information Systems Security Certification Consortium, Inc. ("(ISC)<sup>2</sup>") as follows:

Many public and private sector organizations now recognize the need to cost-effectively protect information systems resources as part of an overall resource management strategy. Information systems security has also come to be seen as more of a people (i.e., behavioral), rather than a technical problem. This has resulted in broad employee security awareness and training efforts in recent years, as well as a proliferation of new organization-specific professional development programs that are intended to "qualify" or "accredit" IS security staff through required training. In total contrast to this apparent "progress" is the recession downsizing in several industry segments that has decimated the ranks of, and in some cases virtually eliminated, many security groups.<sup>1186</sup>

Various professional certification organizations have developed certification programs, including the funds transfer industry,<sup>1187</sup> the legal profession,<sup>1188</sup> and

---

<sup>1184</sup> See Section VIII.D. (Notaries Public), *supra*.

<sup>1185</sup> J. JACOBS, CERTIFICATION AND ACCREDITATION LAW HANDBOOK vii (1992).

<sup>1186</sup> (ISC)<sup>2</sup>, *NEWS from (ISC)<sup>2</sup>* (May 1993).

<sup>1187</sup> See National Automated Clearinghouse Ass'n, *The Accredited ACH Professional Handbook* (1993).

the information security industry. (ISC)<sup>2</sup> has developed a certification program in which, "[i]n addition to demonstrating the requisite experience and subscribing to the ethical code, candidates for the Certified Information Systems Security Professional (CISSP™) credential must pass an examination based on the Common Body of Knowledge (CBK)."<sup>1189</sup>

---

<sup>1188</sup> The American Bar Association accredited six private organizations for the purpose of certifying lawyers as specialists, including in trial advocacy and bankruptcy. The organizations included the National Board of Trial Advocacy and the Commercial Law League of America Academy of Commercial and Bankruptcy Law Specialists. The ABA amended its Model Rules of Professional Conduct in 1992 and subsequently adopted "Standards for Accreditation of Specialty Certifications Programs for Lawyers" in 1993. "The ABA felt that an accreditation mechanism administered by the ABA according to uniform standards would be the most effective way to deal with certification programs." *ABA Denounces New Discovery Rule, Accredits Lawyer Specialization Agencies*, 62 U.S.L.W. 2095 (Aug. 17, 1993).

<sup>1189</sup> There is also an initiative to include within the CBK the proposed "Generally Accepted System Security Principles" ("GSSP"). GSSP are intended to "incorporate the consensus at a particular time as to the practices, conventions, rules, and procedures that information security professionals should employ or that security-related hardware and software products provide to achieve, preserve, and restore the properties of integrity, availability, and confidentiality of systems in their charge." *supra* note 50.



### 3. Products and Services

Accreditation and certification of products and services already plays an important role in the information technology and security industries. For example, *Tempest* testing (for shielding from electromagnetic sensing devices), diverse communications protocol testing and classified community security testing are all well developed. FCA-related products and services that could benefit or already have benefited from testing and validation include algorithms (*e.g.*, for speed), certificate generation hardware and software and relevant systems.<sup>1190</sup>

#### Categories of Products and Services Testing

Testing FCA-related software, hardware and systems can contribute to the reliability of FCA-supported transactions and thereby enhance their legal enforceability and mitigate risk. Two types of testing that are widely recognized for technical assurances are *conformance* testing and *interoperability* testing. Conformance testing verifies that an implementation performs in accordance with a particular specification or standard. While such testing raises confidence in the likelihood that applications will interoperate, it does not in itself ensure interoperability. Interoperability testing, on the other hand, addresses the actual utilization of the subject computer systems. Interoperability testing is performed between two communications/computer platforms, for instance, to assess the ability of two trading partners' EDI systems to communicate and verify their

---

<sup>1190</sup> See *Validated Products List 1994 No. 1 - Programming Languages, Database Language SQL, Graphics, GOSIP, POSIX, Computer Security*, NISTIR 5354 (Jan. 1994). "The testing of Information Technology (IT) Products to determine the degree to which they conform to specific Federal Information Processing Standards (FIPS) may be required by Government agencies as specified by the FIPS, Federal Information Resources Management Regulation (FIRMR) Parts 201-20.303, 201-20.304, and 201-39.1002, and the associated Federal ADP and Telecommunications Standards Index. Products having a current validation certificate or test report may be offered or delivered by vendors in response to requirements as set forth in solicitations by Federal Agencies. The Validated Products List (VPL) contains conformance testing information for [the above-referenced IT Standards]." *Id.* § 1.1, at 1-1.

respective digital signatures effectively.<sup>1191</sup> Such testing by an accredited laboratory offers many advantages, including quality assurance.<sup>1192</sup>

#### **4. National Voluntary Laboratory Accreditation Program**

Standards for interoperability or other testing accreditation for FCA purposes could potentially be developed in conjunction with or, in part, modeled after, the National Voluntary Laboratory Accreditation Program (NVLAP). NVLAP was established in 1976 to accredit laboratories found competent to perform specific tests or types of tests, including conformance tests.<sup>1193</sup> Perhaps the single most critical aspect of an accreditation program is a clear statement of its meaning. The NVLAP Program Handbook includes the following:

NVLAP accreditation signifies recognition of a testing laboratory's competence to perform specific test methods in specified fields of testing. It means that the laboratory's quality system, staff, facilities and equipment, calibration procedures, test methods and procedures, records, and test reports have all been evaluated and found to meet NVLAP criteria. NVLAP accreditation does not mean a guarantee (certification) of laboratory performance or of product test data; it is solely a finding of laboratory competence . . . .

---

<sup>1191</sup> The nature of the FCA is such that interoperability can be separated from issues involving correct operation, vulnerabilities, and performance. The output (or input) is, to a large extent, self-validating. The question is whether the FCA is meeting performance criteria internally.

<sup>1192</sup> See ACCREDITATION PRACTICES FOR INSPECTIONS, TESTING, AND LABORATORIES 22-23 (H. Schock, Jr., ed., 1989) (providing a list of public benefits of national laboratory testing/accreditation).

<sup>1193</sup> NVLAP was established in the Office of the Secretary of Commerce, See 15 C.F.R. § 7, and is a program in Technology Services, Office of Standards Services. Revised NVLAP procedures will appear in 15 C.F.R. § 285.

See 15 C.F.R. § 7; NIST, NVLAP Program Handbook, Computer Network Interface Protocol X.25 3 (NISTIR 89-4036, Mar. 1989) ("NVLAP offers accreditation for specific test methods or types of tests in many areas. NVLAP provides an unbiased third party evaluation and recognition of performance as well as expert technical assistance to upgrade laboratory performance."); see also 35 Fed. Reg. 27,543 (July 21, 1988).



Accreditation does not relieve the laboratory of the need to observe and comply with existing Federal, State, and local statutes, ordinances, or regulations that may be applicable to its operations, including consumer protection and antitrust laws.<sup>1194</sup>

NVLAP procedures for the accreditation of laboratories include detailed requirements for on-site assessment by NIST, meeting with laboratory managers, examining quality assurance systems, documentation, running sample tests, reviewing personnel records and records of periodic internal audits, observing demonstrations of testing techniques and examining major equipment, apparatus and facilities. The FCA could potentially serve as the primary NIST-accredited conformance testing site for FCA-related purposes, or as the beneficiary of such testing (where the testing is provided by a non-FCA entity).<sup>1195</sup>

## 5. Quality Certification and ISO 9000

The ISO 9000 series standards for quality "provide guidance on the selection of an appropriate quality management program (system) for a supplier's operations. [Although] developed primarily for use in two-party contractual situations or for internal auditing . . . [i]n some cases, compliance with one of the ISO 9000 standards (or their equivalent) has been or will be mandated by a U.S., foreign national, or regional government body."<sup>1196</sup>

---

<sup>1194</sup> NVLAP Program Handbook § 3.7. NVLAP does not write technical standards for testing or certification, but sets criteria and standards for accreditation. New NVLAP procedures contain ISO/IEC Guide 25 "General Requirements for the Competence of Calibration and Testing Laboratories" in its entirety. NVLAP is also working to document its compliance with ISO/IEC Guide 58 ("Calibration and Testing Laboratory Accreditation System - General Requirements for Operation and Recognition"). NVLAP will offer auditing of laboratory ISO 9000 compliance.

<sup>1195</sup> See generally ELECTRONIC CONTRACTING, *supra* note 2, § 5-36, at 283-85; see also *id.* §§ 5-31 to -35 (providing an overview of conformance and interoperability testing for EDI and related clearing houses).

<sup>1196</sup> M. Breitenberg, NIST, *ISO 9000 - Questions and Answers on Quality, the ISO 9000 Standard Series, Quality System Registration, and Related Issues*, NISTIR 4721 (1992). However, ISO 9000 does not address the validity of test data. See Int'l Laboratory Accreditation Conf., Committee 1, *Validity of Test Data - The Application of ISO Guide 25 or ISO 9002* (1993).

ISO 9000 can also have an impact on procedures and requirements for cross-certification in the form of mutual recognition agreements among countries for quality assessment<sup>1197</sup>:

As acceptance of ISO 9000 has grown, certification is widely viewed as a stamp of approval. As a result, ISO 9000 is becoming a *de facto* market requirement. This process has gone further in some industries and some countries than in others. For example, in Britain, where the standards have been the most widely embraced, registration has become a virtual necessity for suppliers seeking new business. Over 80 percent of larger employers (payrolls of over 1,000 people) have become registered and even lawyers, doctors and schools are seeking registration.<sup>1198</sup>

In response to the "proliferation of third-party registration bodies in the United States, there is a need for assurance of the competence of those registration bodies so that there can be confidence in the registrations they grant. The Registrar Accreditation Board (RAB) was formed to meet this need in the United States."<sup>1199</sup> The mutual recognition of accreditation boards is also being undertaken to *foster comparability* among registration bodies.<sup>1200</sup> However, it has been noted that "[u]nlike memoranda of understanding, which are relatively long-standing business arrangements, subcontracting usually takes place on an as-needed basis and each registrar maintains an approved list of subcontractors as part of its own quality-assurance criteria. . . . Because subcontractors and auditors operating under memoranda of understanding are not themselves accredited, the

---

<sup>1197</sup> See, e.g., Working Document on Negotiations with Third Countries Concerning the Mutual Recognition of Conformity Assessment (Euro. Comm., 1991); and Communication to the Council on the Negotiation of the Agreements between the European Economic Community and Certain Third Countries on Mutual Recognition in Relation to Conformity Assessment (Euro. Comm., Sept. 21, 1992).

<sup>1198</sup> M. Jenkins, *A look at ISO 9000*, STANDARDIZATION NEWS, July 1993, at 50, 51 (American Society of Testing and Materials).

<sup>1199</sup> Registrar Accreditation Bd., OVERVIEW 1 (1993). "[Additionally] ANSI and the RAB formed the American National Accreditation Program for Registrars of Quality Systems." *Id.*; see 58 Fed. Reg. 39,486 (July 23, 1993) (proposal to establish the National Voluntary Conformity Assessment System Evaluation Program (NVCASE) at NIST).

<sup>1200</sup> See RAB, *supra* note 1199, at 2. Perhaps the issues and structures accommodating mutual recognition deserve scrutiny for their potential value concerning public key cross-certification issues.



registration conferred under these arrangements may carry less weight and may not be as widely accepted as that conferred by an accredited registrar."<sup>1201</sup>

## 6. Certification and Accreditation Liabilities

Certification and accreditation raise legal issues, including the extent to which they warrant subject entities, professionals, or products and services; undertake responsibilities in breach of agreements or with less than the recognized standard of care; and create a restraint in trade.<sup>1202</sup> Also, such organizations will not agree to offer their services without assurances of limited risk.<sup>1203</sup> To the extent that governmental or non-governmental certification and accreditation entities are potentially liable for their acts, the efficacy of agreements that limit liability deserve attention. For example, the following liability disclaimer appears in a standard Underwriters Laboratories "Listing and Follow-Up Service Agreement":

The Subscriber agrees that the Laboratory is performing its functions in accordance with its objects and purposes and does not assume or undertake to discharge any responsibility of the Subscriber to any other party or parties. The Subscriber recognizes that the opinions and findings of the Laboratories represent its judgment given with due consideration to the necessary limitations of practical operation and in accordance with its objects and purposes and agrees that the Laboratory does not warrant or guarantee the correctness of its opinions or that its findings will be recognized or accepted.

## 7. Potential FCA Accreditation and Certification Bodies

On the basis of the foregoing discussion, the following table illustrates an accreditation and certification infrastructure that provides "glue" to ensure that the hierarchy is trustworthy, or otherwise meets user and societal expectations. It is structured as a "top-down" "certification chain" such that:

---

<sup>1201</sup> G. Spizizen, *The ISO 9000 Standards: Creating a Level Playing Field for International Quality*, NAT'L PRODUCTIVITY REV., summer 1992, at 331, 341.

<sup>1202</sup> The precise extent of liability to third parties associated with accreditation and certification entities is uncertain. See J. JACOBS, *supra* note 1185. Note that "a general certification and accreditation scheme was introduced into Danish law" by public notice no. 168 of March 19, 1991. M. Andersen, *The Danish Teletrust-Initiative*, 1 EDI L.R., 43, 51 (1994).

<sup>1203</sup> See ELECTRONIC CONTRACTING, *supra* note 2, § 5.34, at 281.

- a "SECOND-LEVEL CERTIFIER" *develops accreditation/certification criteria, rules and standards. A SECOND-LEVEL CERTIFIER might also consolidate "CERTIFIER" responsibilities;*
- a "CERTIFIER" *tests, evaluates, accredits/certifies SUBJECTS pursuant to such SECOND-LEVEL CERTIFIER criteria;*
- a "SUBJECT" *is an accredited/certified entity within the FCA hierarchy*<sup>1204</sup> (accredited/certified by a Certifier).

For each of these three categories, the following table distinguishes among *private* and *government* environments that might participate in one or more facets of accreditation and certification although, as the table reflects, overlap among private and government parties is inevitable.

Two unrelated examples of hierarchies from which analogies to multi-level certification and accreditation can be constructed are footnoted below.<sup>1205</sup>

---

<sup>1204</sup> The listed FCA/user entities (*i.e.*, TLCA, PCA, CA, ORA) parallel those in the figure describing the MITRE Study's approach except for the two additional entities: "ORG." and "USER." *See* note 12, *supra*.

<sup>1205</sup> **Example 1:** Typical Federal Social Benefits Program.

Congress: Legislation (Overall Policy)  
Reviews Federal Agency Performance

Federal Agency: Develops Program Policies  
Certifies State Compliance

State Agency: Develops Additional Policies  
Certifies County Compliance

County Agency: Develops Additional Policies  
Certifies Beneficiaries

**Example 2:** Some Typical FCA Entity Relationships.

Int'l Standards Body: Develops Standards for High-Level Entities  
Reviews Entity Compliance

TLCA/PRA: Sets Management & Operational Standards  
Reviews PCAs for General Compliance

PCA: Develops Policy for its Own Hierarchy  
Certifies qualified/compliant CA's for each jurisdiction

CA: Administer Policy set by PCA, with appropriate modifications  
Certifies Other Qualified CAs, Orgs., Persons



The following table demonstrates the depth (and inherent complexity) of a comprehensive, multi-dimensional "cradle-to-grave" accreditation and certification scheme. It suggests that considerable strategic planning and continuing resources will be needed to coordinate the many diverse potential accreditation and certification participants. There are invariably additional dimensions to these issues that transcend the artificial boundaries of any such an undertaking. Perhaps most difficult problem, or the greatest weakness of FCA-related accreditation and certification is that there is "no precedent for making [an accreditation] statement about distributed systems. Nobody has done it . . . it is mind boggling and a cause of great frustration."<sup>1206</sup> Consequently, this table represents a mere "snap-shot" of a hypothetical FCA-relevant accreditation and certification environment and is provided solely for pedagogical purposes.

---

LRA: Follows Security Requirements Established by CA  
Identifies Users as Required by CA

Entity: Sub-CA, Organization  
[Person] Receives Certificate

<sup>1206</sup> Telephone Interview with Rob Rosenthal, Mgr. of Protocol Sec. Group, NIST (May 3, 1994). Rosenthal cautioned that "if the standards are not right then conformance to the standards are meaningless . . . the link among business policy and standards is critical and its proper enforcement and integration elusive and yet indispensable." *Id.*

Earlier versions of this table were presented to reviewers for comment. Indeed, this exercise posed considerable difficulty for certain reviewers and the revised table reflects these problems -- the table remains incomplete. This is understandable since the metaphors, proposed architecture, politics and general appreciation of this material is quite difficult; and it continues to evolve. However, because it offers significant challenges (including political ones), it is included despite its "roughness." A table that authoritatively and comprehensively addresses this subject matter will perhaps be capable of completion within a few years, to the extent that it depends upon accreditation and certification entities making considerable progress in the interim.

In examining Table 4, the reader should consider the following: (i) the infrastructure for accreditation and certification may increasingly be a *hybrid* of government and private certifiers and accreditors and therefore the government vs. private separation may diminish in practice; and (ii) to the extent that the (or a) hierarchy is comparatively flat, intermediate level certifiers may either be synonymous with higher-level certifiers or simply nonexistent.

	<b>SUBJECT</b> <i>Accredited/Certified FCA Entity</i>	<b>CERTIFIER</b> <i>Accredits/Certifies Subjects</i>	<b>"2ND-LEVEL" CERTIFIER</b> <i>Develops Accreditation/ Certification Criteria</i>
<b>1. TLCA GOV'T</b>	N/A	EXC; ITU; IPRA	EXC; ISO
<b>2. TLCA PRIVATE</b>	N/A	ITU; IPRA; ANSI	PKAB; USO; ITU; ISO
<b>3. PCA GOV'T</b>	TLCA	DoD; GSA; NIST; USPS	Gov't Agency; EXC
<b>4. PCA PRIVATE</b>	TLCA <i>e.g., IPRA</i>	IPRA; PCB	CAB <i>e.g., Industry Council</i>
<b>5. CA GOV'T</b>	<i>e.g., Comp. System Security PCA Gov't</i>	<i>e.g., System (security) Cert. Responsible Agency</i>	<i>e.g., NCSC/NCSL PCA</i>
<b>6. CA PRIVATE</b>	PCA Private	PCB	PCA
<b>7. ORA GOV'T</b>	CA <i>e.g., PCB; Notary Ass'n</i>	Security Officer/Office	Multi-Agency
<b>8. ORA PRIVATE</b>	CA <i>e.g., PCA or Notary Ass'n</i>	Notary Assn.	CA; External Group
<b>9. ORG. GOV'T</b>	CA, Gov't	Any Subagency	Agency; Gov't
<b>10. ORG. PRIVATE</b>	CA Private <i>e.g., Chamber of Commerce</i>	IA <i>e.g., USCIB</i>	NGO <i>e.g., ICC</i>
<b>11. USER GOV'T</b>	Org. Gov't, CA Agency-Specific	Gov't Contractor; Office	Org.
<b>12. USER PRIVATE</b>	Org. Private; CA <i>e.g., Comp. Sec. Prof.</i>	Org.; PCB; <i>e.g., (ISC)<sup>2</sup></i>	Prof. Org. <i>e.g., ABA, ISSA</i>

**TABLE 4 - ACCREDITATION AND CERTIFICATION MATRIX**



## Abbreviations special to Table 4:

ABV.	FULL NAME	DESCRIPTION
CAB	Commercial Accreditation or Cert. Body	<i>See this Section.</i>
PKAB	Public Key Accreditation Board	Conceived of as a private high-level accred. and cert. board whose directors would include reps. from major private infosec. & trade facilitation groups and users. Or, undertaken within an existing private org. as an adjunct activity.
EXC	Consortia of Exec. Agencies of the U.S. Gov't	Could, <i>e.g.</i> , be administered by NIST as an extension of its current FCA infrastructure coordination.
IA	Industry Association	<i>See this Section.</i>
NGO	Non-governmental Organization	<i>E.g.</i> , An International Org. with U.N. Status
ORG. GOV'T	Government Organization	Public entity with a public key certificate and/or with one or more FCA users.
PCB	Prof. Accredit. or Certification Body	<i>See this Section.</i>
USER, GOV'T	Government User	Includes legal entities, devices or processes within the Org., or independently certified by the CA.

As an example of the structure of Table 4, consider the certification and accreditation of FCA users as described in "12. USER PRIVATE," therein. At the far right of row 12, the ISSA (Information Systems Security Association) serves as the SECOND-LEVEL CERTIFIER in its capacity of developing information systems security certification criteria. The (ISC)<sup>2</sup>, using the ISSA's criteria, then certifies Computer Security Professionals (SUBJECT). This exemplifies a *three-tiered* process of accreditation and certification represented in Table 4 generally.

## 8. Other

There are other noteworthy approaches to mitigate liability among which are education (*see* Recommendation X.Q., *infra*) and implementation of rigorous audit controls.

## B. INSURANCE

### 1. Defined; Purpose

Insurance issues are important for FCA consideration not only as mechanisms for mitigating or apportioning FCA liability, but also as aids in gauging and quantifying FCA responsibilities and financial requirements. Insurance has been

defined as "an arrangement for transferring and distributing risks,"<sup>1207</sup> and an insurance contract has been defined as "an agreement by which one party (usually identified as an insurer) is committed to do something which is of value for another party (usually identified as an insured or a beneficiary) upon the occurrence of some specified contingency."<sup>1208</sup> Broadly defined, insurance can arguably be viewed as encompassing FCA-based public key cryptography in that the underlying FCA infrastructure provides for a transferal and distribution of risk associated with the use of certificate-based digital signatures. This subsection surveys important insurance issues that hold direct relevance to the FCA or that indirectly provide useful structures which can benefit by the thoughtful consideration of approaches to FCA infrastructure.

## 2. Assessing Insurance Risks

A successful program of insurance normally requires a pattern of loss experience, and such a pattern based on actual data is always preferable. Because certification authorities are at an early stage of development, determining the risks associated with the FCA is difficult. Most professionals having engaged in the development of public key cryptosystems will readily recollect hearing or personally espousing the position that "nobody knows the risks involved in public key" (a position also frequently taken by electronic commerce developers).<sup>1209</sup> The following exemplifies the difference between "pure" risk and (statistically) predictable risk:

[S]ince only some portion of the relevant facts that affect any endeavor can ever be known, predictions about the occurrence of a potential loss inevitably are based partly on estimates or guesswork. This speculative aspect is generally understood as the 'element of risk' in an insurance transaction. Recognition of the risk element is essential to developing techniques for managing the unknown and the unknowable, and the transfer of the element of risk in regard to the unknown is the characteristic that is almost invariably associated with any conceptualization of insurance.<sup>1210</sup>

The rule ought perhaps to be that if financial risk to the FCA cannot be adequately assessed, a user "can protect himself by insurance in one form or another if the

---

<sup>1207</sup> KEETON & WIDISS, *supra* note 16, § 1.1(b), at 3. Judge Learned Hand characterized an ideal insurance scheme as "mythically prolix, and fantastically impractical." *Sinram v. Penn. R.R.*, 61 F.2d 767, 771 (2d Cir. 1932).

<sup>1208</sup> KEETON & WIDISS, *supra* note 16, § 1.1(b), at 5.

<sup>1209</sup> But, of course, extrapolation from other areas and actuarial sciences do provide a sound basis upon which to measure unknown risks.

<sup>1210</sup> KEETON & WIDISS, *supra* note 16, § 1.3(a), at 8-9.



risk of nondelivery or error appears to be too great. . . . The company [or the FCA], if it takes out insurance for itself, can do no more than guess at the loss to be avoided."<sup>1211</sup> Risk-taking society depends to a large degree on the capacity of insurance underwriters and their ancillary professionals to assess risks associated with the activity to be insured.<sup>1212</sup> However, the skills and history of practices associated with the sufficient assessment of computer security risk and of the FCA certification process for insurance purposes are in an early stage of development.<sup>1213</sup> Consider the perspective and approach taken by one Lloyd's syndicate<sup>1214</sup>:

Generally, underwriters are not interested in the technicalities of the systems or networks they are covering. They rely upon people like ourselves to indicate whether or not the client takes the appropriate steps to control and secure the activities covered. If significant risks are taken by the client then the underwriters will either decline cover or part cover, or insist that security and control be enhanced to an acceptable level. In terms of high value risks the underwriters can be very powerful in the general improvement of security in particular markets. . . . Therefore, we are inclined towards ensuring that firstly, appropriate procedural and reconciliation controls are in place and then that data is protected during transmission by message authentication and encryption. *Encryption being the lower priority if the transmission is not of a confidential nature.*

---

<sup>1211</sup> Kerr S.S. Co. v. Radio Corp., 157 N.E. 140, 142 (1927).

<sup>1212</sup> One of the oldest and largest insurance companies in the world advertises that, "Correct computer insurance will not be achieved with just a good policy wording. It is even more important to correctly identify the risks and translate them into their insurance implications. To do this requires the marriage of computing and insurance . . ." Brochure of Hogg Group PLC on *Computassure* (1992).

<sup>1213</sup> See Section IX.B.5, *infra* (discussing existing computer and computer security insurance policies).

<sup>1214</sup> "Lloyd's is not an insurance company. It is a society of individuals who underwrite insurance in groups, known as syndicates, but who underwrite for their own account with unlimited individual liability. Each syndicate has a professional underwriter who writes insurance business on behalf of the syndicate members but it is the individuals who provide capital to Lloyd's. It is the members of Lloyd's who receive profits or bear losses." Lloyd's, *Security Underlying Policies Issued at Lloyd's* (Oct. 1991).

EDI is viewed slightly differently since the objective is primarily to minimize human involvement. In these systems insurers [generally] are concerned only about the security of the keys and the key management procedures.<sup>1215</sup>

The approaches to risk evaluation of computer systems by the insurance industry demonstrate a lack of information-technology sophistication. It also suggests that development of a viable and responsive treatment to the FCA-related risks requires further study and development.

### 3. Government Insurance Programs

The federal government operates a number of insurance programs in which insureds pay premiums to the federal government in return for protection from some type of hazard.<sup>1216</sup> These insurance programs are sometimes run through a government corporation chartered for the sole purpose of providing insurance; other times, the federal government operates through private agencies or through subsidies to a governmental unit that serves as the insurer. "[T]he federal government's insurance operations are larger than the combined operation of all the life and property and casualty insurance companies in the United States. . . . Because the federal government is not required to keep the massive reserves that state regulators require private insurance companies to maintain, it has less administrative overhead costs and operates more efficiently. In all probability, every living adult in the United States is covered by at least one federal government insurance program."<sup>1217</sup>

There are various reasons for creating federal government insurance programs, including unavailability of insurance resulting from the unwillingness of private insurers to enter an untested area.<sup>1218</sup> The FCA may fall within the category of "untested areas" and prompt the implementation of a federal insurance program on an experimental basis. This would ordinarily be considered a temporary

---

<sup>1215</sup> Letter from Gerry Grant, WBK International, to Michael S. Baum (Jan. 27, 1993) (emphasis added).

<sup>1216</sup> See B. MITNICK, *THE POLITICAL ECONOMY OF REGULATION* 36 (1980); see also KEETON & WIDISS, *supra* note 16, § 8.6, at 971.

<sup>1217</sup> MITNICK, *supra*, note 1216, at 36-38. Examples of areas in which state or federal governments participate in the insurance business include social security benefits, crop insurance, bank deposit insurance (see Section VIII.A., *supra*), postal insurance (see Section VII.A.4.a., *supra*), and nuclear hazard insurance (discussed *infra*, at text accompanying notes 1219-1221).

<sup>1218</sup> See KEETON & WIDISS, *supra* note 16, § 8.6(c), at 973-79.



activity, but in some instances the problems for private insurers cannot be overcome. For example, in the case of the potentially catastrophic nature of nuclear energy hazards, many private insurers are unwilling to enter the field.<sup>1219</sup> Accordingly, governmental indemnity<sup>1220</sup> for certain nuclear risks has been established as a supplement to the limited amount of private insurance available.<sup>1221</sup>

---

<sup>1219</sup> *See id.*

<sup>1220</sup> *See, e.g.,* Price-Anderson Act, PUB. L. No. 85-256, 71 Stat. 576 (1957).

<sup>1221</sup> In 1967, in the context of amendments to the Price-Anderson Act, Congress "found" the following:

In order to protect the public and to encourage the development of an atomic energy industry, in the interest of the general welfare and of the common defense and security, the United States may make funds available for a portion of the damages suffered by the public from nuclear incidents, and may limit the liability of those persons liable for such losses.

42 U.S.C. § 2012(i).

In pursuance of the foregoing, currently applicable law has established an elaborate scheme for public protection through a combination of public and private means. The following is a brief summary of this scheme, and not all exceptions or subsidiary provisions are covered. Generally, licensees are required to demonstrate "financial protection" to cover liability to the public in an amount equal to that of "liability insurance available from private sources." *Id.* § 2210(a)-(b). This "financial protection" may take a variety of forms, including self-insurance. *Id.* § 2210(b). For those licensees required to hold less than \$560,000,000 of financial protection, section 2210(c) requires the Nuclear Regulatory Commission (the "NRC") to indemnify them to the extent of the difference, to a maximum indemnification amount of \$500,000,000. Aggregate licensee liability to the public is limited to the amount of the licensee's financial protection plus indemnification amounts, if any. *See id.* § 2210(e)(1). To ensure compensation of the public in the event of an "incident," licensees are required to waive any defense of derivative sovereign immunity or the like. *Id.* § 2210(n). In the event the public suffers damage in excess of the liability cap, Congress has directed itself to "thoroughly review" the particular incident and "take whatever action is determined to be necessary (including approval of appropriate compensation plans and appropriation of funds) to provide full and prompt compensation to the public . . ." *Id.* § 2210(e)(2). The NRC's indemnification program is financed in part by assessments against indemnified licensees on the basis of production capacity. *See id.* § 2210(f). Finally, the liability cap was expanded to 7 billion dollars within the 1988 Price-Anderson reauthorization. Pub. L. No. 100-408, 102 Stat. 1066-85 (1988). *Cf.* Convention on Third Party Liability in the Field of Nuclear

Other areas of government activity are supported with forms of government insurance.<sup>1222</sup> The FCA might be a candidate for similar treatment if the risks were considered catastrophic in nature and private insurers were unwilling to enter the field of insurance against FCA hazards.<sup>1223</sup>

Because governmental or quasi-governmental agencies will likely perform many FCA functions, they could be immune from tort liability for FCA functions under the doctrine of sovereign immunity.<sup>1224</sup> Also, when a government agency with partial or complete immunity from liability purchases insurance, an issue arises over whether the insurer, the insured, or both retain a right to invoke sovereign immunity. Government agencies may purchase insurance policies pursuant to agreement that the insured retains discretion to claim an immunity defense. In such cases, the propriety of permitting the insured to claim immunity is "debatable," because the "unpoliced choice" of the insured "invites fraud and chicanery."<sup>1225</sup> The consequence is even less certain when a government agency purchases an insurance policy which is silent regarding the assertion of its immunity as a defense. The majority of state courts have held that the insured

---

Energy (Paris Convention), opened for signature 29 July, 1960 (maximum liability of approximately 15 million SDR), modified by an Additional Protocol signed Jan. 28, 1964 (Brussels Supplementary Convention).

<sup>1222</sup> See generally KEETON & WIDISS, *supra* note 16, § 8.6(b), at 972. For example, the Federal Deposit Insurance Corporation insures the deposits of banks and savings associations; the Federal Flood Insurance Program is operated by the Federal Insurance Administration (see National Flood Insurance Act of 1968, 82 Stat. 572 (1968), 42 U.S.C. §§ 4001-4128); the Federal Crop Insurance Corporation ("FCIC") provides a subsidized all-risk insurance that is serviced by numerous insurance companies pursuant to the Federal Crop Insurance Act (codified at 7 U.S.C. §§ 1501 *et seq.*); and the Small Business Administration (the "SBA") offers the Surety Bond Program. (see 15 U.S.C. §§ 694a *et seq.* ).

<sup>1223</sup> In this regard, inquiry of private insurers has been informally initiated by the author to survey (i) the extent of computer risk policies available, (ii) the extent to which such policies cover CA-related risks, (iii) the need for insurance products expressly covering FCA-related activities, and (iv) the extent of need for federal involvement in the provision of insurance for FCA activities.

<sup>1224</sup> See generally Section VII.A., *supra*.

<sup>1225</sup> KEETON & WIDISS, *supra* note 16, § 4.8, at 383.



and the insurer retain the immunity defense.<sup>1226</sup> However, several jurisdictions have reached a contrary result and have held that purchasing insurance constitutes a waiver of immunity.<sup>1227</sup>

When an insurance contract specifies that the insurer will *not* avail itself of immunity defenses, courts will likely find that the insurer is precluded from asserting the insured's immunity.<sup>1228</sup> Therefore, the FCA will need to consider whether or not it has immunity, whether purchasing insurance will affect this immunity and whether it wants to purchase insurance under these alternative situations.

#### 4. Private Insurance

There are no "standard commercial" policies that *specifically* address certification authorities, although, of course, CA risks might be covered under the agreements of current computer risk insurance. Consequently, it would be prudent to determine the extent to which available insurance policies cover, or might be negotiated to cover, certification authority risk.

As stated above, when an entity purchases insurance, it enters into a contract by which the insurer commits to do something which is of value for the insured upon the occurrence of a specific contingency.<sup>1229</sup> For example, when the insured is liable for negligence, assuming the cause of the negligent injury is covered by liability insurance, the insurer will cover liability up to an established limit. Generally, when an entity purchases insurance, it will select from several different standard coverage policies. However, in some situations, an entity can also arrange for customized insurance coverage. Some insurers specialize in making insurance coverage available that is specially designed to satisfy the

---

<sup>1226</sup> See *id.* at 384 & n.8 (citing *McGrath Bldg. Co. v. City of Bettendorf*, 85 N.W.2d 616 (Iowa 1957); *Mann v. County Bd.*, 98 S.E.2d 515 (Va. 1957); *Kesman v. School Dist.*, 29 A.2d 17 (Pa. 1942)).

<sup>1227</sup> See *id.* at 384 n.9 (citing *Morehouse College v. Russell*, 135 S.E.2d 432 (Ga. 1964); *Geislinger v. Watkins*, 130 N.W.2d 62 (Minn. 1964); *O'Connor v. Boulder Colorado Sanitarium Ass'n*, 96 P.2d 835 (Colo. 1939)).

<sup>1228</sup> See *id.* at 384 n.10 (citing *Stanhope v. Brown County*, 280 N.W.2d 711 (Wis. 1979); *Bollinger v. Schneider*, 381 N.E. 2d 849 (Ill. App. 1978)).

<sup>1229</sup> See *id.*, § 1.1(b) at 4.

unusual needs of the entity insured.<sup>1230</sup> Insurance is almost always available, for a price, provided that the requisite elements of uncertainty and appropriate insurable interest exist.<sup>1231</sup>

## 5. Fidelity Bonds; Errors and Omissions Coverage

Fidelity bond coverage is available to mitigate exposure to employee computer fraud. Some fidelity bonds also carry riders (policy endorsements) insuring against computer fraud perpetrated by non-employees. Also, at least two private insurance carriers currently offer more sophisticated, "stand-alone" computer fraud policies designed to cover the insured against fraudulent transactions. Fidelity bond policies, however, are unlikely to benefit the FCA to the extent it is not a transaction processor. Furthermore, these policies only respond to intentional acts of dishonesty rather than simple errors and omissions.

The Lloyd's Electronic and Computer Crime Policy is one of the few standard policies covering this sort of risk.<sup>1232</sup> Under the Lloyd's policy, the insurer, subject to the terms of the policy, agrees to make good to the insured its direct financial loss sustained under circumstances stated in the policy and occurring and discovered during the period of the policy. The policy covers the insured's loss incurred due to fraudulent input, modification, loss, or destruction of electronic data under specified conditions. The policy also sets forth specific exclusions for losses it does not cover.<sup>1233</sup> The FCA could potentially purchase an insurance

---

<sup>1230</sup> See *id.*, § 2.8, at 128. Lloyd's is famous for being able to customize policies for unusual risks and needs.

<sup>1231</sup> "[T]he insurable interest doctrine requires that there be some significant relationship between the insured and the person, the object, or the activity that is the subject of the insurance transaction." *Id.* § 3.1(b), at 135.

<sup>1232</sup> See Appendix F, *infra* (reprinting relevant portions of the Lloyd's computer policy).

<sup>1233</sup> The Lloyd's policy does not cover, *inter alia*: (a) Loss covered by the insured's Financial institution Bond; (b) Loss caused by employees; (c) Loss of potential income; (d) Indirect or consequential losses; (e) Liability incurred only because it was assumed by insured under contract; (f) Fees incurred by insured to establish the existence of a loss under this policy; (g) Loss due to riots, military, naval or war unless it occurs in transit; (h) Property damage or legal liability for contamination by radioactivity or other hazardous nuclear properties; (i) Loss because of threat to body or property; or (j) Loss of Electronic Data Processing media while in the mail.



policy similar to the Lloyd's policy or have a custom policy drafted for its specific needs if these insurers were willing to enter the FCA insurance field.

Aetna Life and Casualty Company offers Aetna's Computer and Electronic Network Technology Policy (ACCENT). Aetna's policy is similar to that of Lloyd's in that it offers coverage for the introduction of fraudulent data or the fraudulent modification of existing data into or within computer systems and networks owned, operated, and/or used by the insured. Both Aetna's and Lloyd's policies are designed for financial institutions and may therefore have little value to the FCA (unless, of course, financial institutions undertake FCA-like services that are in direct support of their financial services). The Chubb group of insurance companies also offers similar coverage for many types of clients.

A more likely type of private insurance coverage that will benefit the FCA is customized errors and omissions coverage:

An errors-and-omissions policy is professional liability insurance providing a specialized and limited type of coverage compared to general comprehensive insurance [and] is designed to insure members of a particular professional group from liability arising out of the special risks such as negligence, omissions, mistakes and errors inherent in the practice of the profession.<sup>1234</sup>

Although "E&O" policies are typically worded in terms of "any negligent act, error and omission," their coverage can reach negligent performance of contracts as well, as was demonstrated in the data processing field in *Louchette Corp. v. Merchants Material Insurance Co.*<sup>1235</sup> On the other hand, "E&O" coverage does *not* extend to the insured's acts of "legal fraud."<sup>1236</sup> Errors and omissions coverage would protect the FCA from the consequences of its negligent acts, errors and omissions in providing certificate authority or other acts that it may engage in with individual entities.

## 6. Self Insurance

Another possibility is self insurance. If an entity such as a corporation or a government agency engages in a sufficient volume of a specific type of venture,

---

<sup>1234</sup> *Grieb v. Citizens Cas. Co.*, 148 N.W.2d 103, 106 (Wis. 1967) (quoted in 13A G. COUCH, R. ANDERSON & M. RHODES, *COUCH CYCLOPEDIA OF INSURANCE LAW* § 48: 166 at 168 n.11 (2d rev. ed. 1984)) [hereinafter COUCH].

<sup>1235</sup> 429 N.Y.2d 952 (App. Div. 1980) (noted in COUCH, *supra* note 1234, at 167).

<sup>1236</sup> COUCH, *supra* note 1234, § 48:170, at 174 (citing *National Sur. Corp. v. Musgrove*, 310 F.2d 256 (5th Cir. 1962), *cert. denied*, 375 U.S. 974 (1964)).

the enterprise, acting on its own, can spread the risk of all of its individual ventures.<sup>1237</sup> For example, a certification authority could self-insure by allocating a portion of its revenues to a liability claims account or fund.<sup>1238</sup>

A slightly more complicated form of self-insurance is for members of a particular industry to join together in "mutual self-insurance." Law firms, for example, do this in respect of malpractice insurance. Also important in this category are so-called "Protection and Indemnity ("P&I") Clubs" among shippers of cargo.<sup>1239</sup> P&I Clubs are, in general, more cost effective, being mutual and non-profit-making, than cargo insurance companies.<sup>1240</sup> P&I Clubs and similar arrangements work because they are established by a *community of interest* which makes it easier to pool resources. However, it appears that VANs and CAs do not, and will not in the immediate future, be able to conjure up such a community of interest.

*Multibank credits* are another form of spreading risk, and are used to spread credit risk as a matter of prudent banking.<sup>1241</sup> Federal banking regulations include letters of credit for purposes of measuring capital requirements.<sup>1242</sup> Such

---

<sup>1237</sup> See KEETON & WIDISS, *supra* note 16, § 1.3, at 13.

<sup>1238</sup> See *id.* at 14.

<sup>1239</sup> P&I Clubs cover four main types of risk: liability for loss of life and personal injury; liability for loss of or damage to cargo; 1/4 collision liability; and wreck removal, damage to fixed objects, oil pollution, etc.

<sup>1240</sup> Administrative costs of P&I Clubs accounted in 1979 for about 3.5 percent of total claims costs, and 85 to 90 percent of premiums are used for the payment of compensation. An American study, on the other hand, indicates that only about half of cargo insurance companies' premiums go to the payment of compensation, one third covers cost of administration, and the rest is profit. European cargo insurance companies appear to operate with corresponding proportions of 75-20-5 percent. UNCTAD REPORT, *supra* note 1145, at 18.

<sup>1241</sup> See S. Farrar, *Multibank Credits* 525 (Feb. 1, 1988).

<sup>1242</sup> See Federal Reserve Bd., *Proposed Revisions to Capital Adequacy Guidelines* (Draft of Jan. 24, 1988). "A 'standby letter of credit' is any letter of credit, or similar arrangement, however named or described, which represents an obligation to the beneficiary on the part of the issuer (1) to repay money borrowed by or advanced to or for the account of the account party, or (2) to make payment on account of any indebtedness undertaken by the account party, or (3) to make payment on account of any default by the account party in the performance of an obligation." 12 C.F.R. § 32.2(3). Concerning multibank credits and risk sharing, see Ryan,



regulatory schemes provide detailed rules concerning the obligations of participants.

## 7. Conclusion

There are a variety of potential means by which the FCA may be able to obtain insurance for its functions. Before deciding what type of insurance policy to purchase and who will design and underwrite it, the FCA must determine its legal status and whether it has complete or partial governmental immunity for liability. If the FCA has governmental immunity, it may be desirable for it to implement an insurance program in order to provide at least a minimal level of compensation to injured users simply as a matter of "fairness," as well as to bolster its perception of trustworthiness and reliability. Indeed, the perception of trustworthiness and reliability will possibly be of critical importance to determining the FCA's acceptability to the public.

## C. POLICY STATEMENTS AND AGREEMENTS

### 1. Demand for Agreements and Policy Statements

As noted above, the public key environment lacks a legal structure and adequate trade practices, custom and usage or widely-used forms of agreement. Therefore, comprehensive "policy statements" and agreements are indispensable. The need for policy statements and agreements is expressed in many of the critical standards documents and public key infrastructure reports:

- The need for "clearly-articulated" and "well-architected" policies are stated in PEM RFC 1422 as follows:

-It is important that a certificate management infrastructure for use in the Internet community accommodate a range of *clearly-articulated* certification policies for both users and organizations in a *well-architected* fashion. Mechanisms must be provided to enable each user to be aware of the policies governing any certificate which the user may encounter. This requires the introduction and standardization of procedures and conventions that are outside the scope of X.509. <sup>1243</sup>

- RFC 1422 "Outline for PCA Policy Statements" ("PEM Outline") contemplates the use of "legal agreement[s]," as follows:

---

*Letters of Credit Supporting Debt for Borrowed Money: The Standby as Backup*, 100 BANKING L.J. 404, 416-21 (1983), errata corrected in 100 BANKING L.J. 571 (1983).

<sup>1243</sup> PEM RFC 1422, at 1 (1993) (emphasis added).

7. Business Issues- If a legal agreement must be executed between a PCA and the CAs it certifies, reference to that agreement must be noted, but the agreement itself ought not be a part of the policy statement. Similarly, if any fees are charged by the PCA this should be noted, but the fee structure per se ought not be part of this policy statement.<sup>1244</sup>

- RFC 1422 also states, "As part of registration, each PCA will be required to execute a *legal agreement* with the IPRA . . . ."<sup>1245</sup>
- Section X.D., of this Report recommends the development of FCA Agreements and Policies.
- The RSA Commercial Hierarchy requires that "Organizations execute an RSA Commercial Hierarchy legal agreement as a precondition to acceptance by RSA into the Hierarchy."<sup>1246</sup>

Evaluation of the initial PCA Policy Statements that have been promulgated by PEM-based CAs<sup>1247</sup> indicates that the RFC 1422 requirements are probably not legally adequate for much of the contemplated government or commercial use. This is not surprising, given that the PEM Outline upon which all PEM-compliant policy statements are based is purposefully generic, very brief, and largely non-prescriptive. The PEM Outline is perhaps best characterized as a preliminary pioneering attempt to describe important boundaries of a legal infrastructure. However, it was developed without the benefit of input from legal counsel or the traditional process of model agreement (or related) legal policy drafting. Accordingly, it provides an insufficient legal basis for operating an FCA.

Available policies and agreements do not reflect a comprehensive and global evaluation of the legal relationships of all critical parties to the FCA. The following figure illustrates some of the potential parties and their relationships, together with some of the supporting policies and agreements that might be part of a responsive legal environment.<sup>1248</sup> It does not include potentially diverse

---

<sup>1244</sup> The PEM Outline is reproduced in Appendix E.5., *infra*.

<sup>1245</sup> PEM RFC 1422, *supra* note 1243, § 3.4.2.1.

<sup>1246</sup> RSA Data Security, Inc., *Certificate Services* 13 (White Paper July 15, 1993).

<sup>1247</sup> See generally Appendix E., *infra*. (These include those of MIT, RSA, TIS, and COST).

<sup>1248</sup> This figure presents an example of only one of many possible hierarchical approaches to certificate-based public key. Indeed, there remain fundamental disagreements among public key developers concerning architecture. For example, the extent to which cross-certification is permissible and practical



"transactional service" relationships<sup>1249</sup> that are largely viewed as being outside of the FCA's mandate.

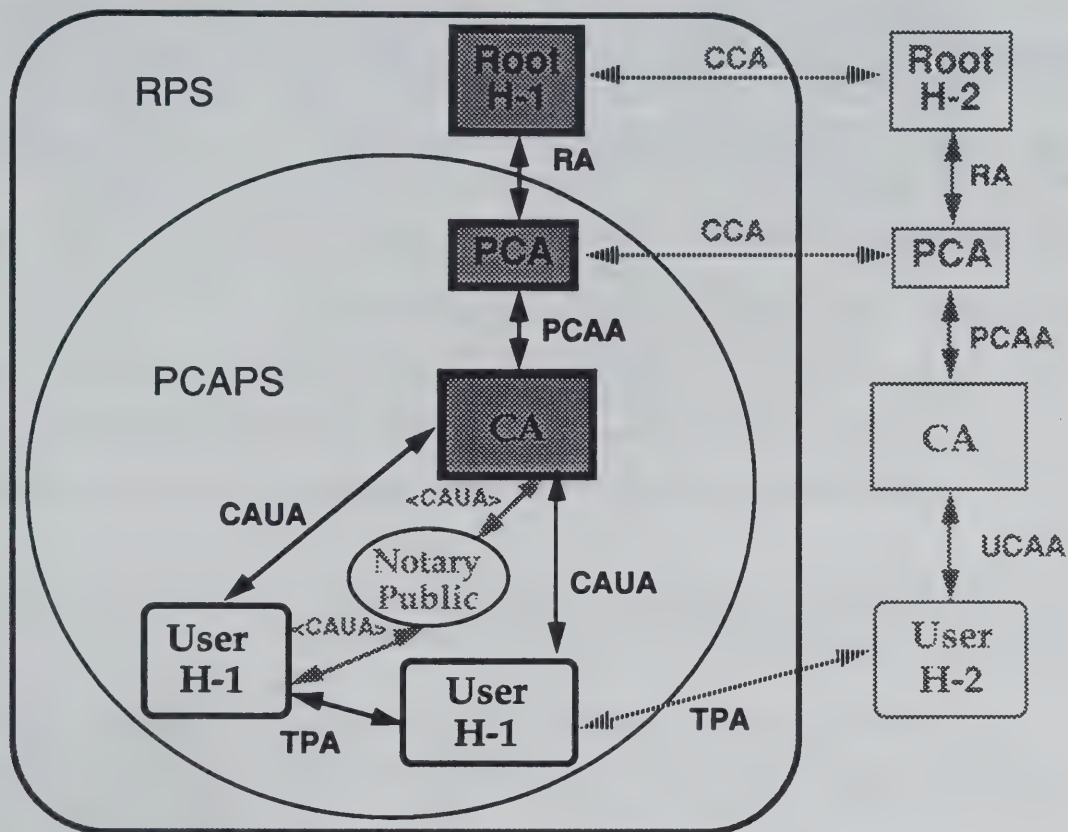


FIGURE 4 - HYPOTHETICAL FCA LEGAL STRUCTURES/RELATIONSHIPS

The above figure contains the following abbreviations for entities:

(because, *e.g.*, of concern that differences in approaches to name subordination might harm or destroy automated digital signature verification); the scope of entities that should constitute the hierarchy (such as, *e.g.*, whether notaries public or time/date stamping services should be viewed as a part of the infrastructure); and the scope of root policy coverage (*e.g.*, whether the root can or will exert control over operational aspects of the hierarchy, or will attempt to minimize its responsibilities and liabilities for damages that extend beyond mere "registration").

<sup>1249</sup> "Transactional" relationships refer to, *e.g.*, the bilateral communications and "business" trade relationships among trading partners.

Root	Registration authority with which all PCA's (or Policy Registration Authorities) within a hierarchy must register/comply.
PCA	Policy Certification Authority.
CA	Certification Authority.
Notary Public	Notary Public - A commissioned public officer of a government. <sup>1250</sup>
User - H1	User in Hierarchy 1 - A User represents either an organization, a person, or both, depending upon the implementation.
User - H2	User in Hierarchy 2.

**TABLE 5 - ENTITIES IDENTIFIED**

The above figure also contains the following abbreviations:

---

<sup>1250</sup> The notary public is included in Figure 4 as an entity that facilitates the binding process, although it need not constitute part of the FCA. *See* Section VIII.D., *supra* (concerning notaries public).



CAUA	CA-User Agreement - Executed among a CA and a FCA user. <sup>1251</sup>
CCA	Cross-Certification Agreement - Executed among entities in different hierarchies. <sup>1252</sup>
PCAA	Policy-CA Agreement - Executed among a Policy CA and subordinate CA.
PCAPS	PCA Policy Statement - Promulgated by a Policy CA; intended to bind all subordinate parties; expected to be consistent with, and provide "flow down" of, applicable RA requirements.
RA	Root Agreement - Executed between the hierarchy's root, <i>e.g.</i> , the Internet Policy Registration Authority (IPRA) and a Policy CA within that hierarchy. This might also be called a "registration" agreement.
RPS	Root Policy Statement - Promulgated by the Root.
TPA	Trading Partner Agreement - Executed among users; may contain electronic commerce terms, <sup>1253</sup> <i>e.g.</i> , those affecting expectational interests concerning digital/certificate signature legal effect. <sup>1254</sup>
TPSPA	Third Party Service Provider Agreement - Executed among an FCA entity or user and a third party service provider. <sup>1255</sup> (not shown in Figure)

**TABLE 6 - POSSIBLE AGREEMENTS AND POLICY STATEMENTS IDENTIFIED**

Unavoidably, the many entities and diverse relationships reflected above in Figure 4 *supra* create a complex environment which requires careful and rigorous

<sup>1251</sup> CAUAs could be used as a temporary measure and will be largely discontinued once trade practices, legislation, or binding "system rules" and policies are available; they will persist longer for "high assurance" PCA purposes, where the perceived risks are great.

<sup>1252</sup> See Section IV.K., *supra*, and accompanying notes (concerning International Root Authorities and cross-certification).

<sup>1253</sup> Trading Partner Agreements are "traditionally" understood to govern bilateral EDI-relevant trade terms. See ELECTRONIC CONTRACTING, *supra* note 2, § 2.6, at 49-105 (defining and analyzing the content of trading partner agreements). Here, the term is used to encompass a broader range of terms affecting computer-based relationships among users.

<sup>1254</sup> See Sections VIII.A.3.-7., *supra* (concerning system rules in the financial services industry that control user-to-user obligations); VIII.B., *supra* (concerning value added networks); and IX.D.2., *infra* (noting an approach to "variation by agreement" of user rights and obligations by "system agreement" in the context of the UNCITRAL draft "EDI Statutory Provisions."

<sup>1255</sup> This table includes TPSPs since TPSPs will likely play an important supportive role for the FCA, *e.g.*, as a message transport mechanism, or more. See Section V.A.2., *supra* (concerning "Communications" as a secondary FCA role).

consideration. Consideration of "battle of the forms" issues should also be a part of the analysis. Each set of relationships among the identified parties must be separately evaluated and supported. Policies and agreements should accommodate these relationships and entities and should articulate the results of such analysis in the text and supporting commentary of such documents. The following figure provides one possible representation of the parties that will be bound to, or otherwise affected by, the identified policies and agreements. An "X" indicates that the respective parties will directly execute and be bound; an "O" that the respective parties will (or may) be affected by, or otherwise bound, in the absence of privity.<sup>1256</sup>

AGREEMENT OR POLICY (OF H-1)	RA	PCAA	PS	CAUA	CCA	TPA	TPSPA
ENTITY:							
Root - H1	X				X		X
PCA - H1	X	X	X		X		X
CA - H1	O	X	O	X	O		X
User 1 - H1	O	O	O	X	O	X	X
User 2 - H1	O	O	O		O	X	X
Root - H2	X				X		X
PCA - H2	O	O	O		X		X
CA - H2	O	O	O		O		X
User - H2	O	O	O	X	O	X	X
Notary Public				O			X

TABLE 7 - POSSIBLE COVERAGE OF POLICIES AND AGREEMENTS

The above relationships and coverage of policies and agreements is tentative and intended solely for pedagogical purposes.

## 2. Policy Statements

In some certificate-based public key infrastructures, such as PEM, responsibilities and the apportionment of liability are intended to be governed by the use of policy statements. Because PEM structures appear to be influencing the direction of the FCA infrastructure, the scope and content of the PCA Policy Statements being promulgated pursuant to RFC 1422 Section 3.4.3 ("Policy Certification Authorities") deserve close scrutiny.<sup>1257</sup> The PEM Outline requires that eight

<sup>1256</sup> The binding effect of non-bilateral written agreements is considered generally in Sections IX.D.2., *infra*.

<sup>1257</sup> Recommendation X.D. *infra*, assumes that NIST will recommend the adoption of a PEM-like approach to PCAs and PCA policy statements.



subject areas be addressed in a policy statement: (1) PCA identity, (2) PCA scope, (3) PCA security and privacy, (4) certification policy, (5) CRL management, (6) naming conventions, (7) business issues and (8) "other." The scope and treatment of these issues in policy statements provides a window on the risks and obligations associated with the operation of such infrastructures. The following table summarizes the critical content of the available draft, proposed, or issued policy statements on the basis of the high-level criteria noted in the PEM Outline and other relevant criteria.<sup>1258</sup>

ENTITY:	Massachusetts Institute of Technology	RSA Data Security, Inc.	Trusted Information Systems, Inc.	COST International Consortium
ISSUE:	<i>See App. E.1</i>	<i>See App. E.2</i>	<i>See App. E.3</i>	<i>See App. E.4</i>
Name of Policy	"Midrange" Policy for Unaffiliated Individuals	"Low Assurance" Certification Authority Policy Statement	PCA Policy Statement	Cost Consortium Policy Statement
Policy Date	Experimental	[August 11, 1993]	July 1, 1993	January 1, 1993
L PCA IDENTITY				
1.1. Distinguished Name	[C=US; ST=MA; O=Massachusetts Institute of Technology; OU=MIT PCA]	C=US; O= RSA Data Security, Inc.; OU= Low Assurance Certification Authority	[C=US/ST=MD/ O=Trusted Information Systems PCA/] [OU=Residential CA/]	C=SE O=Computer Security Technologies CST AB

<sup>1258</sup> The PEM Outline is reprinted in Appendix E.5., *infra*. Table 8 uses the following conventions:

- Each of the eight PEM Outline categories is listed in shaded text.
- Requirements for each category specified in the PEM Outline are listed below each category, respectively.
- Additional descriptions that do not explicitly appear in the Outline are italicized.
- Information about the four listed PCA Policy Statements that was not included in the PCA Policy Statement but was instead obtained directly from the subject PCAs is framed in [brackets].

The author does not represent that either the appended PCA policy statements or the information contained in this table are accurate and current. This information is provided for discussion purposes only.

<b>1.2. Postal Address</b>	[MIT Policy Cert. Auth. MIT Rm. E40-311 1 Amherst St. Cambridge, MA 02139 USA]	[RSA Certificate Services 100 Marine Pkwy. Suite 500 Redwood Cty, CA 94403 USA]	[T.I.S.] 3060 Wash. Rd. Glenwood, MD 20738 USA	[Cost Computer Security Tech. AB Barnhemsvagen 12 16576 Hasselby, Sweden]
<b>1.3. E-mail</b>	[mit-pca@mit.edu]	[pca-info@rsa.com]	tis-pca@tis.com	cost-pem@cost.dsv.su.se
<b>1.4. Phone</b>	[1-617- 253-8400]	1-800-PUBLIK-E	1-301-854-6889	[+46-8-16 16 92]
<b>1.5. Policy Validity Period</b>	[Until Revised (Policy will be re-signed at least once per year)]	[One Year]	[Until Revised]	[Until Revised]
<b>2. PCA SCOPE</b>				
<b>2.1. Community Served</b>	Educational & Business	Unrestricted, incl. anonymous or persona	Educational, business gov. [& residential] worldwide (incl. residential)	[Unrestricted, worldwide (except US & Canada), incl. residential]
<b>3. PCA SECURITY &amp; PRIVACY</b>				
<b>3.1. Technical &amp; Procedural Security Measures to Protect Generation &amp; Protection of PCA Key Components</b>	PCA will use appropriate hardware <i>e.g.</i> , BBN SafeKeyper	Best efforts; info. stored on "generally unsecured server"	Good faith effort	[Two access passwords, secret keys encrypted, smart card in v. 2.0 (Jan. 1994)]
<b>3.2. Security Requirements Imposed on CAs and Users</b>	Good faith efforts to protect private component & to identify individuals prior to certification; to use own discretion	Reasonable measures; largely a local matter	Reasonable hardware, software, phys. & procedural methods to protect priv. key	[For CAs, the same as for PCA; for users secret keys encrypted on Diskettes (PC & MAC) Smart Card in v.2.0 (Jan. 1994)]
<b>3.3. Info. Privacy Regime</b>				
<b>3.4. Req. Cert. Generation Hardware by CAs?</b>	No	No	[No]	[Not required; Smart Cards will be available in v.2.0]
<b>4. CERTIFICATION POLICY</b>				
<b>4.1. Policy &amp; Procedures to Certify CAs</b>	[CA or indiv; Alt.: any Edu. Inst. (undecided)]	Any CA or individual	TIS right to judge "legitimacy and uniqueness" of name	Only lower level PCAs & CAs using COST-PEM software
<b>4.2. How Policy Applies Transitively to Users &amp; Subordinates</b>	Good faith efforts to properly identify end-users	Subject names subordinate to issuer name & end-users cannot issue certificates	Proced. for issuance that give "reasonable" assurances of DN's ident ok & subord.	[Secret key protection is same for PCA, smart card will be available; not required]



4.3. Is User Affiliation to a CA Required (where CA Required to Cert. only Affiliated Users)?	Yes; Authorization to act on behalf of org. not implied.	No	[Yes, except for residential]	[Local matter of the CA]
4.4. Procedures to Resolve DN Conflicts	"More specific info. & proof of incorporation or equivalent"	Check against data base for duplicate valid certificate; for persona: first come, first serve		[Unique CA's DN required, unique user's DN within CA's domain required.]
4.5. Locally Defined Conventions ok?	Yes, to clarify affiliation: e.g., OU= guest		[DNs must be descriptive and unique]	[Yes, no special requirement]
4.6. CA Cert. Validity Restrictions	$\geq 6$ mo. $\leq 2$ yrs.	1 mo. $< > 2$ yrs.	$[\geq 3$ months and $\leq 2$ years]	$\leq 2$ yrs.
4.7. Issuance Time Limits on Cert. Start Time	[Validity starts when PCA signs, no pre- or post-dating]	7 days prior $>< 60$ after request	[Validity starts when PCA signs, no pre- or post-dating]	[None]
4.8. Restrictions on End-User Certificates Issued by CAs	None	[End-users cannot issue certificates]		
5. CRL MANAGEMENT				
5.1. Frequency of CRL Issuance	[Monthly]	Monthly	Advertised basis	N/A - kept by CAs as the local CRL db.
5.2. Constraints on frequency of CRL issuance by its CAs	None	Monthly	None	[None: CRLs updated contin. & immed. avail.]
5.3. Other Constraints on Subordinate CAs	None			[Name of lowest (user) CA must be cost-pem@<local-domain>]
5.4. PCA CRL Mailbox	[crl-service@mit.edu]	[crl-storage@RSA.com]	tis-pca-crl@tis.com	[cost-int@cost.dsv.su.se]
5.5. CRL Inquiry Mailbox	[crl-service@mit.edu]	[crl-retrieval@rsa.com]	tis-pca-crl@tis.com	[CA/PCA mail address]
5.6. Procedures for Invoking Additional CRL Mgt. Services	Requested Acks. of CRL request honored	Requested Acks. of CRL request honored		[Built-in COST-PEM User Agents: request certificate, retrieve certificate]
5.7. Mandatory CRL Services by CAs	[Undetermined, but will be non-profit]	Push CRLs to PCA initially & periodically		[Storage of CRLs]
5.8. Archive Server: Push or Pull (not required by 1422)	Pull by CAs/users to confirm receipt	[Pushed to IPRA (for PCA and Persona)]	CAs push to PCA	Kept by local CA for reply to specific user requests
6. NAMING CONVENTIONS				

6.1. Special Conventions		None	Reasonable assurances of Disting. name.	[DN constructed from E-mail address]
6.2. Subordination (DN Subordination not an option in 1422, rather part of common policy)	Must be subordinate to the CAs DN	Subordinate to issuer; not viol. trademarks; for persona: subor. to issuer name, contain one extra term commonName attribute	CA must only issue certificates with subordinate DNs	Subordinate to COST; Per RFCs
6.3. Semantics				
7. BUSINESS ISSUES				
7.1. Limitation on Liability	Without warranty	[N/A]	Without warranty	All possible efforts to assist and correct [Funct.& Correctness (describ. in Manuals) guaran'd, provided oper. (platform) reqs. are met by user]
7.2. Disclaimer of Warranty	AS IS	None	AS IS	None
7.3. Patents	No grant of right to use public key technology	RSA Licensed Implementations only	No implied licenses by use of PCA	N/A
7.4. Written Agreement Between PCA and CAs	Optional Agt.: limited to affirmation of warranty disclaimer	[N/A]	CAs must execute licensing agt.; limited to affirmation of lack of warranty	Yes
7.5. Fees	\$XXX for revoc. & reissuance	Registration fee for each CA; & revoc. fee; no fee for persona cert.	See schedule of fees in appendix	\$2,000 - CA \$400 - PEM agent work station
8. OTHER				
8.1.	CA may have only one valid cert. w/ this CA, with exception.	Procedures are provided for certification of end-users.	TIS reserves right to inspect CA records for naming compliance	[operational; Claims: "HIGH ASSURANCE" [per 3.1 & name binding & issuer ident guar.]

**TABLE 8 - POLICY STATEMENTS COMPARED**

The information in Table 8 demonstrates that PCA Policy Statements issued pursuant to the RFC 1422 mandate do not exhibit the clarity, consistency and



practical useability needed for FCA purposes, at least from a legal perspective.<sup>1259</sup> Consequently, a model PCA Policy Statement for FCA purposes is needed.

### 3. Model Policy Statement Development

Model PCA Policy Statement development is needed because a PEM-like model (or at least a hierarchical model) appears most likely to be adopted for certain FCA purposes. In addition to the above reasons, the need for model PCA Policy Statement development is considerable and includes the following:

- **Existing Policy Statements/Infrastructure are Inadequate:** As noted above, the scope and content of existing PCA Policy Statements promulgated pursuant to RFC 1422 are inadequate to serve many of the purposes for which the FCA is intended to serve.
- **Policy Statement Longevity:** Because policy statements are intended to remain in effect for long periods of time without modification, the need for rigorous drafting and resolution of issues is particularly acute. The need for an "immutable" policy is reflected in the PEM Outline as follows:

8. Other- Any other topics the PCA deems relevant to a statement of its policy can be included. However, the PCA should be aware that a policy statement is considered to be an immutable, long lived document and thus considerable care should be exercised in deciding what material is to be included in the statement.

- **Ancillary Documents do not Substitute for Model Policy Statements:** For example, although the American Bar Association's draft Global Public Key Infrastructure Rules of Practice ("ABA Rules")<sup>1260</sup> are intended to provide a legal framework for certificate-based public key cryptography, the ABA Rules do not substitute for a Model PCA Policy Statement (hereinafter a "Model Policy") because the ABA Rules (1) are intended to be generic and articulate high-level principles; (2) address both private and public sector activities (whereas the Model Policy should comprehensively address government activity); and (3) will not necessarily take positions that are always consistent with federal interests, and therefore may not fully satisfy FCA infrastructural needs.

---

<sup>1259</sup> Review of the above promulgated policies indicates a lack of consistent treatment of these categories in terms of depth, ordering, terminology and content.

<sup>1260</sup> See Section IX.D.1., *infra*.

- **Disinterested Party Draftsmanship:** Cooperation, fairness and consensus in drafting viable model legal documents is indispensable and can best be assured when drafted within a neutral and objective forum and by a "neutral party" that is mandated to seek consensus among the interested parties, rather than by a particular expectant federal agency PCA that may desire to influence PCA policy to its benefit. Future PCA policy statements developed as a by-product of federal agency-specific public key initiatives are inadequate because the needs of anticipated FCA users are eclectic, particularly in an inter-agency environment.
- **Comprehensive Coverage:** Such a model should be rigorously drafted; address many issues not covered, or inadequately covered, in RFC 1422; contain appropriate options; and provide relevant and useful references and commentary. The Model Policy should adopt positions that provide an appropriate balance of interests among the FCA and its users.

#### 4. Model Agreements

Agreements are needed to govern and improve the certainty of the rights and obligations of various FCA entities, users and, applicable interconnected non-FCA service providers. Because of the relative detail comprised in a formal agreement (as compared to the generality of current PCA policy statements), and because of a prudent concern for assuring maximum legal certainty with respect to FCA activities, the development of model FCA agreements is important.

This position is consistent with this Report's recommendation that:

In the absence of [legislation], written agreements expressly setting forth appropriate liability schemes, warranties and the like will need to be utilized, at least until FCA policies are further developed and are recognized as binding on all applicable parties. Although case law suggests the unenforceability of certain such provisions in various instances, they are an important and responsible alternative to legislation.<sup>1261</sup>

The development of model agreements will be valuable, whether or not such models are actually implemented,<sup>1262</sup> and will most likely prove indispensable to the development of:

---

<sup>1261</sup> Model agreement development will also advance other recommendations urged herein, such as for the development of *Legal Goals in Criteria for FCA Pilots*. See Section X.B., *infra*.

<sup>1262</sup> For example, the Foreword to the ABA's *Model Electronic Payments Agreement and Commentary* states that "In addition to providing a sample agreement structure, the Agreement and the associated comments are intended to be an educational tool and strategic planning guide for trading partners



- a primary educational publication that will help users and providers climb the admittedly steep learning curve,
- a clear and complete articulation of the parties' legal rights and obligations,
- a systematic, analytical approach to operational issues of importance on a day-to-day level,
- an "actualized" encapsulation of the current knowledge and practices, and, hence,
- a document that can easily be comprehended and will reveal gaps and flaws more readily than abstract policy analysis.

## 5. Conclusion

The development of model PCA policy statements and agreements will efficiently fill a critical gap in FCA infrastructure development and will have the collateral effect of improving technical infrastructural development. Models will assure that a range of policy and security issues are properly articulated such that they may be intelligently and systematically developed. The development of the FCA cannot leave an indispensable component (such as policies and agreements) to chance. In recognition of the all-too-well-understood fact that a chain is only as strong as its weakest link, policy and agreement development should be handled accordingly.

The creation of quality and practical models requires rigorous analysis, extensive consultation and consensus-building with all relevant parties. Indeed, experience with model EDI agreement development demonstrates that quality draftsmanship is a time-intensive undertaking.<sup>1263</sup> An initial step will be to

---

considering the implementation of electronic payments. The Agreement highlights major issues trading partners should consider and understand . . . ." MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, *supra* note 2, at 26.

<sup>1263</sup> It is time-intensive both in terms of the consultation process -- soliciting and waiting for responsive comments from affected parties, which typically requires multiple consultations with various parties to obtain feed-back on incrementally mature drafts -- and also in terms of the research and drafting of the text and commentary itself. Clearly, model agreements in the public key arena will be pioneering and will therefore require supporting commentary to assist users in understanding their obligations and to provide guidance for the actors in dispute resolution mechanisms, such as judges and arbitrators.

determine (1) which relationships create the greatest risks; (2) the adequacy of policy statements versus agreements for each of the relationships; and (3) a strategy for ensuring that all applicable relationships of those identified above in Figure 4, are addressed. Finally, each "higher level" policy statement and agreement should seek seamless integration with one another, and should be drafted to be as brief and simple to understand as possible without loss of operative effect or meaning.<sup>1264</sup>

---

<sup>1264</sup> A goal could be established to keep Models within practical page limitations. Also, flexible and alternative approaches could be provided, such as the use of incorporation by reference of "master agreements or policies," coding of terms for brevity, and the use of "system rules." See Section IX.D.2.d., *infra* ("System Rules").



## D. MISCELLANEOUS INITIATIVES

### 1. Draft ABA Model Global Public Key Infrastructure Rules of Practice

The Information Security Committee, EDI and Information Technology Division, Section of Science and Technology of the American Bar Association has undertaken a project to develop *Model Global Public Key Infrastructure Rules of Practice* ("Global Rules").<sup>1265</sup> The rules will include risk of loss provisions and seek to fill a gap in the existing literature and legal infrastructure.

### 2. UNCITRAL EDI Statutory Provisions

The United Nations Commission on International Trade Law ("UNCITRAL")<sup>1266</sup> Working Group on Electronic Data Interchange (the "Working Group")<sup>1267</sup> is

---

<sup>1265</sup> The Global Rules do the following:

1. Adopt a cradle-to-grave organizational approach;
2. Accommodate diverse, yet "typical" business transactions ("business" includes government transactions);
3. Include many variant and optional provisions to accommodate diverse applications and implementations;
4. Address user rights and responsibilities within a business context;
5. Assume a hierarchical model;
6. Accommodate both domestic and international use;
7. Contemplate and accommodate diverse standards and algorithms;
8. Address computer-based business transactions in general; *i.e.*, not limited to electronic data interchange (EDI) transactions;
9. Are an educational tool, containing introductory material, and extensive commentary and annotation;
10. Contemplate the development of a "relative minimum essential set of standards" and a "barebones template;"
11. Address, among other issues, "authorization" but not "persona" certificates;
12. Address the authentication of digitally signed archival records; and
13. Contemplate the development of future legislative proposals.

Information Sec. Comm., ABA, *Tentative Scope of Guidelines* [Global Rules] (Oct. 8, 1993).

<sup>1266</sup> UNCITRAL was established by the United Nations General Assembly in response to a perceived need to remove international trade barriers. Resolution No. 2205 (XXI) of Dec. 17, 1966. UNCITRAL's mandate includes "[p]reparing or promoting the adoption of new international conventions, model laws and uniform laws and promoting the codification and wider acceptance of

developing "EDI Statutory Provisions" (the "Draft Statutory Provisions" or "Draft Rules")<sup>1268</sup> to accommodate the use of EDI in international trade.<sup>1269</sup> Although it

---

international trade terms, provisions, customs and practices, in collaboration, where appropriate, with the organizations operating in this field." *Id.* ¶ 8(c).

<sup>1267</sup> In 1992, the Working Group was mandated to draft legal rules on the basis of preliminary studies on the legal issues of EDI considered by the Commission in 1990 and 1991. It was formerly known as the Working Group on International Payments at the time when it was preparing the UNCITRAL Model Law on International Credit Transfers. *See* Report of the United Nations Commission on International Trade Law on the work of its 25th sess. Official Records of the General Assembly, 47th sess., Supp. No. 17 (A/47/17) (1992), ¶¶ 140-148.

<sup>1268</sup> The initial proposal regarding preparation of model statutory provisions was made by the UNCITRAL Working Group on International Payments in a report on the work of its 24th sess. (A/CN.9/360) (1991), ¶ 129. At a later stage, "[i]t was observed that a more flexible term [than 'model law'] was needed in order to reflect that the text contained a variety of provisions relating to existing rules scattered throughout various parts of different national laws in a typical enacting State. It was thus a possibility that enacting States would not necessarily incorporate the text as a whole and that the provisions of the model law would not necessarily appear together in any one particular place in the national law." UNCITRAL, Report of the Working Group on Electronic Data Interchange on the work of its 27th sess. (A/CN.9/390) (Apr. 12, 1994), ¶ 17, at 6 [hereinafter Working Group Report of Apr. 1994].

<sup>1269</sup> The precise scope of the Draft Rules remains uncertain. However, the Draft Rules will tentatively accommodate a "Data [record] [message]" which has been proposed to mean "information created, stored or communicated by electronic, optical or analogous means including, but not limited to electronic data interchange (EDI), telegram, telex or telecopy." Revised articles of draft uniform rules on the legal aspects of electronic data interchange (EDI) and related means of data communication (A/CN.9/WG.IV/WP.60) (Jan. 24, 1994), art. 2(a), and Working Group Report of Apr. 1994, *supra* note<sup>1268</sup>, ¶ 45, at 11. It was also noted that "the aim of the uniform rules should be to encompass the broadest possible range of techniques, whether readily available or still to be developed," Report of the Working Group on Electronic Data Interchange on the work of its 26th sess. (A/CN.9/387) (Nov. 17, 1993) [hereinafter Working Group Report of Nov. 1993], but "should not apply to purely oral communications." *Id.*, ¶ 37, at 10. The Draft Rules are intended to accommodate diverse computer-based trade practices, just as the FCA is intended to accommodate diverse uses. *See* Sections IV.F., (assumption that the FCA will accommodate diverse transactions); IV.I., (assumption that the FCA must support security of interconnected networks



is unlikely at this stage that the Draft Rules will *specifically* address either cryptographic methods of authentication or certification authorities, the Draft Rules, as well as UNCITRAL's recently adopted "Model Law on International Credit Transfers" (the "Model Law"),<sup>1270</sup> address important information security issues and requirements to which the FCA should give due consideration.<sup>1271</sup> Relevant information security issues that may be incorporated into the Draft Rules and that are relevant to the FCA are surveyed below, and include proposals that would confirm the parties' ability to agree on the implementation of even substandard or unreasonable security procedures and that would sanction the use of "system rules" (e.g., rules contained within TPSP-user agreements)<sup>1272</sup> by end users in their computer-based transactions.

### a. Security Requirements

The Working Group has engaged in a detailed inquiry and debate concerning the Draft Statutory Provisions' requirements for security procedures.<sup>1273</sup> At the highest level, the pivotal issue for both the Statutory Provisions and the FCA concerns the duty of the parties to provide and adhere to a specified level or strength of security. This issue concerns whether the duty is to provide security that is no greater than that used by other similarly situated users, or whether the duty is greater, perhaps even extending to the use of state-of-the-art technologies and techniques. Although there is no clear consensus on the duty to be established, a rough articulation of the possible spectrum of security requirements is described in the following table. Each of the listed security standards represents

---

internationally), *supra*; cf. Section X.C., *infra* (recommendation urging the study and development of legislative proposals).

<sup>1270</sup> Adopted by UNCITRAL on May 15, 1992 and subsequently approved by the General Assembly in its annual resolution reviewing the work of UNCITRAL, Resolution 47/34 of Nov. 25, 1992.

<sup>1271</sup> Some legal observers perceive a trend in international legal reform initiatives to catalyze, greatly influence or, in some cases, preempt domestic law reform. This is particularly evident with regard to the law of documentary credits. See Section VIII.G.4.-6., *supra*.

<sup>1272</sup> The corresponding relevant FCA documents are, of course, PCA policy statements and FCA agreements. See Section IX.C. ("Policy Statements and Agreements"), *supra*.

<sup>1273</sup> See *Linking Security*, *supra* note 2, § II.b., at 37-39 (concerning requirements for "reasonable security procedures"); see also Section VIII.A.2. ("Article 4A"), *supra*.

incrementally stronger levels of security, with commercial usage the weakest and "best available" the strongest. Because the relative ordering of the specified security requirements/standards is in dispute, the table is presented simply as an analytical starting point.

LEVEL OR STRENGTH OF SECURITY:	LOWER			HIGHER
STANDARD OF CARE:	"Commercial Usage"	"Appropriate Security" ---- "Appropriate Under the Circumstances"	"[Commercially] Reasonable Security" (CRS) <sup>1274</sup>	"Best Available Security"
COMMENT:	At least as good as that used by others similarly situated; the lowest common denominator	Determination of "appropriate" may include national legislative interpretation	Flexible; question is not whether security is the best available; potentially requires more than current industry practice	May approach state-of-the-art; or at least provide more than CRS

TABLE 9 - SECURITY REQUIREMENTS COMPARED

As a practical matter, there is general agreement that any security standard must simultaneously not over burden commerce with procedures, and be meaningful and practical to implement. Each of the above security requirements<sup>1275</sup> is considered in more detail below and reflects comments and positions advanced by the Working Group's delegates (as well as by delegates of the UNCITRAL Working Group on International Payments in the context of the preparation of the UNCITRAL Model Law on International Credit Transfers) in support of, or

<sup>1274</sup> "Commercially" is bracketed to reflect certain of the Working Group's delegates' preference for a "reasonable security" rather than a "*commercially* reasonable security" standard. See Working Group Report of Nov. 1993, *supra* note 1269, ¶ 85, at 20.

<sup>1275</sup> As a possible addition to the above table, consider "due diligence," which has been advocated as an "objective" standard representing an undertaking of those security measures that are commensurate with the risk in a particular industry. Compare the security obligations imposed by one telecommunications provider: "Customer must make *every reasonable effort* to safeguard the Card number . . ." AT&T, *Terms and Conditions for Using the AT&T Card* (1993), § 11 (emphasis added).



against each, proposed security requirement, as supplemented by other relevant material.<sup>1276</sup>

### **"Commercial Usage"**

Support: Conformity to "commercial usage" is a well known concept in commercial legislation and within the European Commission.

Criticism: "Commercial usage," as well as "commercially reasonable security," are excessively "vague." Also, some regulators assert that a "commercial usage" standard may concede too much control to commercial parties.

### **"Appropriate Security; Appropriate Under the Circumstances"**

One delegation proposed a standard of "technically appropriate." With respect to "appropriate under the circumstances," it was noted that the use of the expression "in the circumstances" in the Model Law on International Credit Transfers was a "last minute addition" and is confusing. Article 5(c) of that Model Law states, "The parties are not permitted to agree that a purported sender is bound under paragraph 2 if the authentication is not commercially reasonable in the circumstances." Accordingly, it was suggested that the expression be kept in brackets to make it optional. Another delegation urged the adoption of a standard of "method sufficient under the circumstances" and permitting national law to make provision for what "type of authentication is sufficient" under such a standard.<sup>1277</sup>

### **"Commercially Reasonable Security (CRS) "**

Support: Whereas CRS is described in the above table as a "higher" level of security, one delegate stated that "the notion of 'commercial reasonableness' is useful in that it may provide a minimum standard of authentication to be

---

<sup>1276</sup> In keeping with Working Group protocol, the particular delegations by whom these comments and positions were advanced are not identified.

<sup>1277</sup> One delegate noted that: "The actual requirement is not inconsistent with Justice Stewart's statement [in *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964)] concerning pornography in that it is not easily defined but, 'I know it when I see it.' Business people make decisions daily without looking to statutes to determine what technologies to use. Business does not know how to conform to such standards."

complied with in the absence of other requirements resulting from contractual arrangements or regulatory requirements."<sup>1278</sup> Another delegate proposed that CRS is no less clear in meaning than "reliability:"

"In practice, the commercial reasonableness of an authentication procedure depended on factors related to the individual payment order, such as whether the payment order was paper-based, oral, telex or data transfer, the amount of the payment order and the identity of the purported sender, and any statements of the parties in their agreement that they chose to use a procedure that was less protective than others available, especially if they explained the reasons why they had made that decision. The Model Law should not discourage the use of a given method of authentication for the sole reason that it would be less secure than other methods available, particularly if the receiving bank offered the sender at a reasonable price another authentication procedure that clearly was commercially reasonable, but the sender chose to use the less secure procedure for reasons of its own. . . ." <sup>1279</sup>

In determining whether a method of authentication was commercially reasonable, factors to be taken into account might include the following: (1) the status and relative economic size of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions took place between the parties; (4) the kind and size of the transaction; (5) the status and function of signature in a given statutory and regulatory environment; (6) the capability of the communication system; (7) the authentication procedures set forth by communication system operators; and (8) any other relevant factors.<sup>1280</sup>

Criticism: Negative comments included the following: "A standard of commercially reasonable security will not achieve the purpose of greater conformity. It is therefore a matter for national governments." "'Commercially Reasonable Security' is broad and vague;" and "Although we can use 'commercially reasonable' as a starting point, it may not have built up enough usage to be meaningful." Compare the following comment:

[A]s long as there would be no case law to determine the content of a commercially reasonable method of authentication, parties could have no certainty as to the legal

---

<sup>1278</sup> Report of the Working Group in Electronic Data Interchange (EDI) on the work of its 25th sess. (New York, Jan. 4-15, 1993), A/CN.9/373 (Mar. 9, 1993) [hereinafter Working Group Report of Mar. 1993], ¶ 68, at 18. As an historical note, the issue of whether the parties could agree to include *no* security was not resolved by the Working Group on International Payments.

<sup>1279</sup> Report of the United Nations Commission on International Trade Law on the work of its 24th sess. (June 10-28, 1991), General Assembly, Official Records: 46th sess., Supp. No. 17 (A/46/17) (Aug. 28, 1991), ¶ 110, at 28.

<sup>1280</sup> Working Group Report of Mar. 1993, *supra* note 1278, ¶ 67, at 17.



validity of the agreements they might enter into regarding methods of authentication.<sup>1281</sup>

Meaning of Commercially: It was noted, for example, that Canada "does not have a qualifier of 'commercially' reasonable security, therefore, [the Statutory Provisions should] adopt a standard without that qualifier, such as 'reasonable security', or 'reasonable under the circumstances'." One delegate was at a loss as to what "commercial" added to a standard of reasonable security or usage, and suggested that the Draft Rules not adopt a standard of "commercial usage:"

The objectiveness of a criterion based on 'commercial reasonableness' was also said to be questionable [because it] might result in increased uncertainty as to what methods of authentication would be regarded as acceptable in any given jurisdiction. [And] the use of the word 'commercial' might create an undesirable dichotomy between the 'commercial' uses of EDI and other business uses of EDI involving parties that might, in certain jurisdictions, not be regarded as conducting a 'commercial' activity (e.g., certain categories of professionals).<sup>1282</sup>

Meaning of Reasonable: It was suggested that the term "reasonable" is unknown in civil law systems and has been criticized in Mexico where there is no jurisprudence on the matter. Another delegation did not object to the term "reasonable":

A view was expressed that the term 'commercially reasonable' . . . was too vague a standard for measuring the adequacy of authentication methods. It was stated that additional precision would be obtained by adding the words 'safe and' before the words 'commercially reasonable' . . . The Commission concluded that those types of qualifying words were not appropriate since the concepts of safety and reliability were themselves an integral part of the notion of commercial reasonableness. A view was expressed that, under some circumstances, parties might reasonably agree to have no security because of commercial considerations. Another proposal was to include in the provision factors to be taken into account in assessing whether an authentication procedure met the standard. There was general agreement with the basic thrust of the proposal; yet, as the proposed factors related to the circumstances surrounding a credit transfer, the Commission decided that it would suffice to add the words 'under the circumstances' after the words 'the authentication method provided is.'<sup>1283</sup>

---

<sup>1281</sup> Discussion preliminary to the adoption of the UNCITRAL Model Law on International Credit Transfers, UNCITRAL, Report of the 24th sess. (June 1991), *supra* note 1279, ¶ 110, at 28.

<sup>1282</sup> Working Group Report of Mar. 1993, *supra* note 1278, ¶ 70. at 18.

<sup>1283</sup> Discussion preliminary to the adoption of the UNCITRAL Model Law on International Credit Transfers, UNCITRAL, Report of the 24th sess. (June 1991), *supra* note 1279, ¶ 106, at 27.

It is clear that none of the above standards enjoys a common, recognized meaning either internationally or among the various member states, and that the extent of such requirements vary. Consequently, it was suggested that uniform interpretation might be best served by choosing a security standard that did not already have special significance within a particular delegation's legal system and was therefore neutral and would resist national interpretation. The Working Group would thus provide, *ab initio*, a new standard with a precise meaning. In this way, confusion and misunderstanding would be minimized, but not, of course, eliminated.

It is proposed by the author that the adoption of a lower, as compared to a higher, security standard cannot convincingly be linked with diminished barriers to ubiquitous computer-based trade because the adoption of a lower versus a higher standard is, in fact, a "double-edged sword," as described in the following table.

	LOWER SECURITY STANDARD	HIGHER SECURITY STANDARD
<b>BENEFIT:</b>	Lower implementation costs (requiring less sophistication to implement); greater access to trading partners who do not have (or use) enhanced security techniques and practices.	Greater real and perceived trustworthiness encourages use for an expanded scope of applications; better accommodates <i>critical</i> transactions. Greater provability/enforceability; reduced risks.
<b>COST:</b>	Lower trustworthiness, elevated fear of sensitive data disclosure and unenforcability; tends to limit use to noncritical transactions; potentially higher losses & insurance costs; data redundancy costs; more conventional controls needed. <sup>1284</sup>	Greater implementation costs; <sup>1285</sup> greater educational requirements/learning curve to implement; reduced access to trading partners who do not have (or use) enhanced security techniques & practices.

TABLE 10 - COSTS AND BENEFITS OF SECURITY STANDARDS

---

<sup>1284</sup> "Self-imposed data redundancy" means that the parties create and retain paper copies or re-transmitted computer-based records of communications as a precautionary measure against errors and fraud.

<sup>1285</sup> See LINKING SECURITY, *supra* note 2, § III.b., at 52 tbl. 4 ("Survey of Costs in Implementing Cryptography"). Note, however, that end-to-end cryptographic security is increasingly embedded in operating systems (with a resulting lower cost) and other software and is increasingly transparent and "user friendly."



## Financial vs. Non-Financial Security Standards

Approaches to the apportionment of liability within the Model Law and U.C.C. Article 4A (on fund transfers)<sup>1286</sup> (collectively "Financial Rules") are useful foundational materials for the development of a practical FCA liability scheme. Although the Financial Rules are limited to *financial* electronic transfers, they are detailed, adopt a "reasonable security procedures" standard and address many issues relevant to electronic commerce generally. However, important distinguishing characteristics among financial and non-financial environments make clear differentiation between financial and non-financial standards necessary so that the FCA's security and liability scheme may take a position that properly and beneficially reflects these similarities and differences accordingly. The following table distinguishes three critical environments (financial, EDI and FCA) as reflected by their requirements. The differences support the adoption of electronic commerce and FCA security standards that are justifiably distinct from the approaches taken in the Financial Rules.

---

<sup>1286</sup> See Section VIII.A.2. ("U.C.C. Article 4A"), *supra*.

FINANCIAL RULES	EDI RULES	FCA RULES
Focused exclusively on financial applications and transactions.	Focused on diverse applications and transactions, including satisfying general contract formation obligations.	Focused primarily on government applications and transactions, although seeking to accommodate commercial needs.
Addresses both user-bank and bank-bank security and liability.	Addresses user (trading partner-trading partner) liability.	Addresses FCA-entity liability; yet, "system rules" may potentially be included, addressing end-to-end (trade) issues.
Historically geared towards relatively closed and proprietary communications environments.	Geared toward direct connect and extensive use of VANS; some "open EDI" contemplated.	Geared toward open systems, multi-networked environments and "open trading."
Did not contemplate the use of public key security services.	Contemplates the use of diverse levels and types of security, although password/User-ID predominantly accommodated.	Focused on the use of public key cryptography and diverse strong security services, including, <i>e.g.</i> , <i>non-repudiation</i> .
Generally skewed toward banking interests, as reflected by their relationships with funds transfer systems.	More "user oriented" than Financial Rules; focused on VANs rather than banks as intermediaries.	Rules intended to achieve a fair balance of interests. However, government-based agreements are generally non-negotiable.
Purpose of security: to authenticate transactions.	Purpose of security: to authenticate transactions or to satisfy "functional equivalent" requirements such as for writings & signatures.	Purpose of security: to support trusted infrastructure for strong authentication and nonrepudiation of transactions for diverse applications.
Trade usage: extensive before the advent of Financial Rules.	Trade usage: developing, although not necessarily identifiable due to diversity of implementations and usage.	Trade usage: largely nonexistent; yet contemplated reliance on FIPS, guidelines, and policy statements.

TABLE 11 - FINANCIAL , EDI AND FCA ENVIRONMENTS COMPARED

### Security Requirements of Various Legal Structures

The security standards of care required by specified legislation, rules, regulations and model agreements are presented in the following table. This table demonstrates a lack of consistency and meaning concerning security requirements and highlights yet another dimension of the challenge.<sup>1287</sup> Nonetheless, the table is not meant to suggest either that there may or may not be legitimate reasons to vary the requirements from one area of the law to another.

<sup>1287</sup> See LINKING SECURITY, *supra* note 2, § III.c., at 54-59 (presenting a model security baseline).



CONVENTION, RULE, REGULATION, MODEL AGREEMENT	SECURITY DEFINITION	PRIMARY SECURITY APPLICATION	CITE
ABA Model EDI Trading Partner Agt.	"Reasonably sufficient"	EDI	§ 1.4.
ABA Model Electronic Payments Agreement	"reasonable security procedures"	Financial EDI; EDI	§ 7.1
CMI Rules for Electronic Bills of Lading	"Reasonable Care"	Electronic Bills of Lading	Art. 9.c.
U.C.C. Art. 4A	"Commercially Reasonable"	Fund Transfers	U.C.C. § 4A-202
UCP 500 - Documentary Credits	"Reasonable Care"	Docu. Credits	Art. 13
UN Convention on the Liability of Operators of Transport Terminals in International Trade	"all measures that could reasonably be required to avoid the occurrence and its consequences"	Cargo	Art. 5
UNCITRAL Model Law on Int'l Credit Transfers	"Commercially Reasonable"	Fund Transfers	Art. 5(a)
International Telecommunications Union Constitution	"methods and procedures which practical operating experience has shown to be the best"	Telecom-munications	Art. 27(2).

**TABLE 11 - SURVEY OF SECURITY DEFINITIONS**

#### **b. Variation by Agreement - Party Autonomy**

No matter which of the above security requirements is adopted, an important underlying issue concerns whether the parties should be permitted the freedom to vary security requirements and the apportionment of liability by agreeing to implement *unreasonable* or *inappropriate* security. Restated, to what extent should "party autonomy" be sanctioned? The party autonomy issue is inextricably linked to public policy considerations which will significantly affect Draft Rules development. At an earlier meeting,

[t]he Working Party was generally agreed that the uniform rules should contain a general recognition of party autonomy. However, it was also agreed that in formulating individual provisions of the uniform rules the Working Group would, in accordance with public policies and with the need to maintain fair relations in EDI, consider the need for limiting the freedom of parties to deviate by agreement from a provision. It was pointed out that, to the extent the uniform rules would deal with the relationship between EDI networks and users of their services, there might be a need to protect the interests of parties that were in a weaker bargaining position.<sup>1288</sup>

---

<sup>1288</sup> Working Group Report of Mar. 1993, *supra* note 1278, ¶ 37, at 10.

As a matter of perspective, the Model Law contains a general recognition of party autonomy.<sup>1289</sup> Similarly, a proposed version of the Draft Rules provides: "[e]xcept as otherwise provided in these rules, the rights and obligations of the [sender] [originator] and the addressee of a data [record] [message] arising out of these Rules may be varied by their agreement."<sup>1290</sup>

At the Working Group's meeting in January of 1993:

[a] suggestion was to distinguish between the situation in which EDI users were linked by a communication agreement and the situation in which parties had no prior contractual relationship regarding the use of EDI. Where parties were linked by a communication agreement, messages should be regarded as authentic provided that the parties had agreed on a commercially reasonable method of authentication and they had complied with that method. *In the absence of a communication agreement between the parties, a*

---

1289 "Except as otherwise provided in this law, the rights and obligations of parties to a credit transfer may be varied by their agreement." MODEL LAW, *supra* note 1270, art. 4. See R. Bhala, *Paying for the Deal: An Analysis of Wire Transfer Law and International Financial Market Interest Groups*, 42 KAN. L. REV. (spring 1994) (urging variation by agreement of funds transfer law by system rules). Cf. U.C.C. § 4-103(a), which permits parties to vary the terms of Article 4:

by agreement, but the parties to the agreement cannot disclaim a bank's responsibility for its lack of good faith or failure to exercise ordinary care or limit the measure of damages for the lack or failure. However, the parties may determine by agreement the standards by which the bank's responsibility is to be measured if those standards are not manifestly unreasonable.

U.C.C. § 4-103(a). See Hal Scott, *New Payment Systems: A Report to the 3-4-8 Committee of the Permanent Editorial Board for the Uniform Commercial Code* 40 (1978) (considering system rule variance affect on third parties).

1290 Revised articles of draft uniform rules on the legal aspects of electronic data interchange (EDI) and related means of data communication (A/CN.9/WG.IV/WP.60) (Jan. 24, 1994), at art. 5. Also, art. 10(4) of the Draft Statutory Provisions considers party autonomy issues:

The [sender] [originator] and the addressee of a data [record] [message] are permitted to agree that an addressee may be deemed to have approved the data [record] [message] although the authentication is not [commercially] reasonable in the circumstances.

*Id.* art. 10(3).



message should be regarded as authentic provided that it was authenticated by a method that was commercially reasonable under the circumstances.<sup>1291</sup>

As the Working Group deliberations reflected:

[t]here was general support for the principle of party autonomy . . . Differing views were expressed, however, as to how the principle should be implemented in the uniform rules. Under one view, which supported the working of the draft article, the emphasis should be placed on the general principle of party autonomy, which should prevail unless otherwise expressly stated by the uniform rules.<sup>1292</sup>

The Working Group also noted that "[T]he uniform rules should ensure, that, as between themselves, parties relying on the use of EDI were free to allocate the risks and to agree on a limitation of their liability with respect to either direct or indirect damage that might result from the use of EDI."<sup>1293</sup>

In further considering the propriety of party autonomy, other suggestions of various Working Group delegates concluded that "it is not possible [to permit the parties] to agree on 'not commercially reasonable'," and that "[p]arties cannot make an agreement against commercially reasonable security." Other delegates proposed "complete party autonomy." It was also noted that "[y]ou cannot say that the parties can do things unreasonably. Rather the agreement is *per se* reasonable and we should not look beyond it. Furthermore, consideration must be given to the impact of complete party autonomy of consumers."<sup>1294</sup>

---

<sup>1291</sup> Working Group Report of Mar. 1993, *supra* note 1278, ¶ 67, at 17-18 (emphasis added).

<sup>1292</sup> Working Group Report of Nov. 1993, *supra* note 1269, ¶ 74, at 18.

<sup>1293</sup> Working Group Report of Mar. 1993, *supra* note 1278, ¶ 148, at 31-32. The "general support for the principle of party autonomy" was restated by the Working Party at its 27th sess. in New York (Feb. 28-Mar. 11, 1994). Working Group Report of Apr. 1994, *supra* note 1268, ¶ 74, at 18.

<sup>1294</sup> The quoted comments appear in the author's notes of interventions by delegates, Working Group on EDI, UNCITRAL (Vienna, Oct. 1993). Subsequently, "[t]he Working Group reaffirmed the decision made at its nineteenth session that the model statutory provisions should apply to all messages, including messages to or from consumers, but that it should be made clear that the model statutory provisions were not intended to override any consumer protection law (see A/CN.9/373), ¶¶ 29-31." Working Group Report of Apr. 1994, *supra* note 1268, ¶ 39, at 10.

Because reliability and trustworthiness are fundamental to an effective computer-based infrastructure, it is advanced that, at a minimum, the parties to trade transactions should act in a commercially reasonable manner.<sup>1295</sup> Such a position promotes an ascertainable "baseline" level of trustworthiness. Consequently, the Statutory Provisions and the FCA should adopt a position to the effect that the sender and recipient are not permitted to agree that a purported sender is bound if the authentication is not reasonable in the circumstances.<sup>1296</sup> Not inconsistent with this position,

[i]t was stated that the uniform rules might, to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. It was recalled that such well-established rules were normally of a mandatory nature since they generally reflected decisions of public policy. A concern was thus expressed that an unqualified statement regarding the freedom of parties to derogate from the uniform rules might be misinterpreted as allowing parties, through a derogation to the uniform rules, to derogate from mandatory rules adopted for public policy reasons. It was thus suggested that . . . the uniform rules should be regarded as stating the minimum acceptable form requirement and should, for that reason, be regarded as mandatory, unless they expressly stated otherwise.<sup>1297</sup>

---

<sup>1295</sup> See Baum, *Position Paper on UNCITRAL Draft EDI Rules*, Working Party on EDI, Int'l Chamber of Commerce, Doc. No. 460-10/7 (Sept. 29, 1993).

<sup>1296</sup> See *id.*

<sup>1297</sup> Working Group Report of Nov. 1993, *supra* note 1269, ¶ 64, at 15; Working Group Report of Apr. 1994, *supra* note 1268, ¶ 75, at 18.



## Third Party Beneficiaries

If the parties are permitted to agree that a purported sender is bound in the absence of a commercially reasonable authentication, the harm to the bound party in a fraudulent transaction is potentially considerable, particularly in the case of interested third parties.<sup>1298</sup> By way of example, consider the case where a bankrupt company is alleged to have entered into a computer-based contract when the security procedures implemented are unreasonable but nonetheless agreed upon by the parties. The trustee in bankruptcy who later seeks to evaluate the claim of the counterparty may be unable to prove any problems of the purported transfer. In this example, the third party beneficiaries (the trustee and other creditors) are affected by the conduct of the sender and recipient and yet cannot otherwise exert control over such transactions.<sup>1299</sup>

### c. System Rules Issues

The party autonomy issues extend to "system rules" issues, which potentially affect information security requirements to a considerable degree. System rules issues refer to provisions within intermediary<sup>1300</sup> and VAN agreements that

---

<sup>1298</sup> See LINKING SECURITY, *supra* note 2, § III.b., at 54 (considering various transactions and corresponding effects on third party beneficiaries as the "primary beneficiar[ies] of security").

<sup>1299</sup> It must be remembered, however, that the third party beneficiary problem is inherent in most commercial transactions, whether traditional or computer-based.

<sup>1300</sup> Intermediary has been defined as meaning "any person who, as an ordinary part of its business, engages in receiving data [records] [messages] covered by these Rules and forwarding such data [records] to their addressees or to other intermediaries. [An intermediary may, in addition, perform such functions as, *inter alia*, formatting, translating, recording, preserving and storing data [records] [messages]." Draft Statutory Provisions, UNCITRAL A/CN.9/WG.IV/WP.60 (Jan. 24, 1994), art. 2(e). One delegate urged that "party autonomy should apply not only in the context of relationships between originators and addresses of data records, but also in the context of relationships involving intermediaries. Working Group Report of Apr. 1994, *supra* note 1268 ¶ 62, at 15.

The definition has undergone considerable debate. For example, it was suggested "that the definition of an 'intermediary' should not be made dependent upon whether an intermediary performs its functions 'as an ordinary part of its business'." Working Group Report of Nov. 1993, *supra* note 1269, ¶ 49 at 12. "It was agreed that the definition should also take into account other possible

prescribe the obligations *among the users* of that TPSP or VAN. The Draft Rules permit senders and recipients to vary their rights and obligations by agreement but do not include a provision that expressly recognizes the effect of "system rules" in varying the parties' respective rights and obligations. In other words, the Draft Rules do not consider the efficacy of a VAN agreement that includes operative provisions that control the otherwise bilateral obligations of trading partners.<sup>1301</sup> This limitation potentially restricts "open-EDI" and may diminish confidence in the enforceability of certain user-oriented provisions contained within FCA policy statements and agreements. However,

[i]t was pointed out by the proponents of that view that, in addition to direct agreements between senders and recipients of trade data messages, agreements concluded with intermediaries and, in particular, *contractual system rules* established by network operators would need to be accommodated.<sup>1302</sup>

The "system rules" debate reflects concern over the relative bargaining power of the parties:<sup>1303</sup>

---

functions an intermediary might perform, such as recording, storing, preserving or translating data." *Id.* ¶ 50. Indeed, "the list of possible services in the definition [is] non-exhaustive." Report of the Working Group on Electronic Data Interchange on the Work of its 27th sess. (A/CN.9/390) (Apr. 12, 1994) ¶ 62 at 15.

It was noted that the definition of intermediary in the Model Law did not expressly exclude the sender and the recipient of a specific message from being an intermediary. Notwithstanding, it was suggested that "the uniform rules should focus on the validation of a transaction concluded between the end points of the transmission chain. Such an approach might lead to minimizing, in relative terms, the role of intermediaries that were not parties to that transaction." Report of the Working Group on Electronic Data Interchange on the Work of its 26th sess. (A/CN.9/387) (Nov. 17, 1993), ¶ 51, at 12.

<sup>1301</sup> Cf. U.C.C. § 4A-501 (providing that "a funds-transfer system rule governing rights and obligations between participating banks using the system may be effective even if the rule conflicts with this Article and indirectly affects another party to the funds transfer who does not consent to the rule."). Also, compare the role of the EDI functional acknowledgments, where "[t]he prevailing view, however, was that the uniform rules should, to the extent possible, avoid dealing with the contractual relationship between value-added networks and their users." Working Group Report of Nov. 1993, *supra* note 1269, ¶ 137, at 32..

<sup>1302</sup> *Id.* ¶ 63, at 15 (emphasis added).

<sup>1303</sup> See Section VIII.B. ("Value Added Networks"), *supra*.



since contracts between network operators and their customers are almost always prepared by the network operators and, with rare exceptions involving large customers, the network operators will not negotiate special terms with their customers, these contracts present a classic example of contracts of adhesion. The uniform rules might, therefore, provide for some means of ascertaining the fairness of the contract terms and the extent to which they would be enforceable. Such a means might be specific to the uniform rules or might partake of more general means of controlling contracts of adhesion.<sup>1304</sup>

It has been urged that:

[i]t is true that the present UNCITRAL rules as they stand do not devote enough interest to the growing role of intermediaries, a term which may refer to VANS . . . But before considering such a potentially dangerous provision such as "these rules may be varied by applicable third party service provider rules", which could ruin any default rules carefully designed for parties having neglected to sign an interchange agreement between them, the very purpose of a model -law-, don't you think it is high time to look deeper into the functions of the so-called intermediaries, a vague term for a lot of varied jobs?<sup>1305</sup>

By extending Article 5 of the Draft Rules to include variation of agreement by system rules, the FCA will be better accommodated. The propriety of the use of "system rules" between a user and an intermediary to govern user-to-user relationships is fertile ground for analysis and action.<sup>1306</sup>

### 3. Security-Relevant Standards

The International Standards Organization (ISO), the International Telecommunications Union (ITU), the Accredited Standards Committee X3 (ASC X3), the Accredited Standards Committee X9 (ASC X9), the Accredited Standards Committee X12 (ASC X12), the European Computer Manufacturers Association

---

<sup>1304</sup> UNCITRAL, Working Group on Electronic Data Interchange, Outline of possible uniform rules on the legal aspects of electronic data interchange (EDI), 25th sess. (New York, Jan. 4-15, 1993), A/CN.9/WG.IV/WP.55 (Nov. 27, 1992), ¶ 29, at 9.

<sup>1305</sup> Fax from Mme. Anne de la Presle, Services du Premier Ministre, France, to Michael Baum (Oct. 26, 1993).

<sup>1306</sup> TPSPs and the FCA may, in fact, provide a unique solution in extending commercial usage and thereby promote electronic commerce. *See Sinclair Oil Corp. v. Sylvan State Bank*, 869 P.2d 675, 676 (Kan. 1994) (considering the applicability of ACH RULES and Fed. Reserve Bank Operating Letter No. 12 "where the initiating party is not a financial institution and is not a party" thereto.).

(ECMA) and the Economic Commission for Europe, Working Party 4 (UN/ECE/WP.4), among other regional, national and international standards-making entities, include information security-related standards that are relevant to the FCA.<sup>1307</sup> Additionally, FIPS PUBS require agencies to "employ risk management techniques to determine the appropriate mix of security controls needed to protect specific data and systems. The selection of controls shall take into account procedures required under applicable laws and regulations . . . . Optional tools and techniques for implementation of security and authentication may be provided by ASC X12 and UN/ECE/WP.4 for use in connection with their respective families of standards."<sup>1308</sup>

#### 4. Alternative Dispute Resolution Mechanisms

The costs of traditional litigation could be overwhelming to the FCA and to non-government entities, such as the Internet Policy Registration Authority ("IPRA"), even were the FCA or IPRA ultimately to prevail. Consequently, alternative dispute resolution ("ADR") mechanisms and, in particular, binding arbitration,<sup>1309</sup> are considered because of their potential to mitigate liability by reducing dispute resolution administrative and legal expenses and potentially by catalyzing agreement among the parties. The use of ADR has been considered, and to an extent, promoted for electronic commerce disputes among trading partners.<sup>1310</sup> ADR for public key infrastructural and transactional disputes deserves further study.<sup>1311</sup>

---

<sup>1307</sup> See M. Baum, *The Proposed Digital Signature Standard: Implications for Electronic Data Interchange*, 8 COMPUTER L. & SEC. REP. (Sept.-Oct. 1992) (surveying security initiatives undertaken by these entities).

<sup>1308</sup> FIPS PUB 161 (on EDI).

<sup>1309</sup> The Standard Arbitration Clause of the American Arbitration Association ("AAA") provides:

Any controversy or claim arising out of or related to this contract, or the breach thereof, shall be settled by arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association, and judgment upon the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

AAA, *Commercial Arbitration Rules* 5 (1991). The AAA "is a public-service, not-for-profit organization offering a broad range of dispute resolution services to business executives, attorneys, individuals, trade associations, unions, management, consumers, families, communities, and *all levels of government*." *Id.* at 4. (emphasis added).



## X. CONCLUSIONS AND RECOMMENDATIONS

As noted from time to time throughout this Report, few decisions regarding the FCA's infrastructure have been made. The consequent lack of definition has opened the field of inquiry to a considerable extent and permits the consideration of many options. By the same token, however, this lack of definition inhibits the formation of specific conclusions and recommendations to a substantial degree. The following recommendations are accordingly general in nature and are subject to revision as planning proceeds.

*Please see the following pages for the detailed conclusions and recommendations.*

---

For international disputes, the International Chamber of Commerce provides Rules of Arbitration and an International Court of Arbitration. *See* International Chamber of Commerce, *ICC Rules of Conciliation and Arbitration*, Pub. No. 447-2 (1992). "The world-wide reputation of the ICC International Court of Arbitration has continued to grow, nourished by the experience and expertise gathered in the course of handling some 7,000 cases involving international commercial disputes since the Court was established in 1923." *Id.* at Foreword.

<sup>1310</sup> *See, e.g.*, MODEL ELECTRONIC PAYMENTS AGREEMENT, *supra* note 2, § 11.5 (providing optionally for the use of the AAA's Commercial Arbitration Rules). To the extent that the FCA may desire the development of case law to provide greater certainty, the usefulness of ADR is limited. For this reason, the first published version of the United Kingdom's EDI trading partner agreement did not include an arbitration clause. *See* ELECTRONIC CONTRACTING, *supra* note 2, § 2.40, at 99-100.

<sup>1311</sup> In this regard, the author has proposed to the Computer Disputes Resolution Committee of the AAA that it respond to the developing requirements of public key infrastructure by offering corresponding services. The ICC's International Court of Arbitration might also provide benefit to parties within an international setting.

## **A. FORGE AHEAD WITH AN FCA IMPLEMENTATION**

The federal government should proceed with the development and implementation of the FCA and should assign one or more entities to do so rapidly. Liability is controllable if specific legislation is enacted. In the absence of the foregoing, written agreements expressly setting forth appropriate liability schemes, warranties and the like will need to be utilized, at least until FCA policies<sup>1312</sup> are further developed and are recognized as binding<sup>1313</sup> on all applicable parties. Although case law suggests the unenforceability of certain such provisions in various instances,<sup>1314</sup> they are an important and responsible alternative to legislation. However, it must be recognized that it is the courts rather than the pilots that will ultimately test legal mechanisms.

## **B. INCLUDE LEGAL GOALS IN CRITERIA FOR FCA PILOTS**

FCA pilots should seek the development of mechanisms to facilitate the satisfaction of various legal requirements and should seek to maximize legal experience. By way of example, and not as a specific recommendation, such legal requirements might include satisfaction of criteria intended to produce computer-based analogs of signatures, notarial acknowledgments and negotiability, as well as other specific requirements of specialized business and government documents. The experience gained from pilot(s) is indispensable in the development of PCA policy statements, model agreements and legislation.

## **C. PROMOTE THE STUDY AND DEVELOPMENT OF LEGISLATIVE PROPOSALS**

Existing legislation and regulations fail to provide the specificity and certainty desirable for a ubiquitous and fully functional FCA. In particular, the Federal Tort Claims Act should be revisited to address FCA activities specifically. On the one hand, to the extent that currently effective exceptions to FTCA liability are not applicable, and it has been seen that they are largely not, the FCA faces potential liability for the *foreseeable* consequences of its negligence.<sup>1315</sup> This, needless to say, is an unacceptable risk. On the other hand, to the extent that the "postal

---

<sup>1312</sup> On policies generally, *see* Section IX.C., *supra*.

<sup>1313</sup> *See* Section VI.B., *supra*.

<sup>1314</sup> *See generally* Section VI.D., *supra*.

<sup>1315</sup> The FTCA is considered in Section VII.A.3.a, *supra*. The "postal matter" exemption from liability under the FTCA is discussed at Section VII.A.4.a., *supra*.



matter" and "misrepresentation" exceptions to FTCA liability *are* applicable, the consequent total exemption from liability would be inconsistent with this Report's conception of optimal "trusted entity" functionality. Recognizing that the enactment of legislation and the development of related regulations will likely take at least several years, it is recommended that this process be commenced in the near term.

#### D. DEVELOP FCA AGREEMENTS AND POLICIES

Given the current and prospective lack of a responsive and robust legal infrastructure, NIST should urge, and appropriately participate in, the development of FCA agreements and policies expressly governing the relationships among FCA users, CAs, PCAs and any TLCA. Until certain electronic commerce legal issues become more settled, agreements and policies constitute the most effective means for providing certainty as to legal rights and obligations and predictability as to the consequences of their violation. It cannot be over-emphasized, however, that courts have a variety of means available to them of ignoring contract terms, particularly those addressing liability limitations.

These agreements can be crafted in both "short" and "long" forms to facilitate various policies, uses and implementations of the FCA. Related agreement and policy *facilitation projects* could include the development of recognized data codes that represent FCA legal agreement clauses and policies. Such codes could be used to enhance the machine-processability of the certificate application process, perhaps in a manner consistent with various code lists developed for electronic commerce.<sup>1316</sup>

---

<sup>1316</sup> The code corresponding to representations and certifications under the FAR are examples of such data codes, and could include something comparable to the proposed "EDITERMS" under development within the International Chamber of Commerce. EDITERMS are defined as "Alpa-numeric codes - from two to ten units - meant to be used when concluding a contract between commercial enterprises or with a government administration, in order to define the respective obligations of each of the parties concerning the modalities of the electronic exchange of data related to the said operation, with reference to a pre-established catalogue recognized as carrying weight among the trading interests concerned." J. Huet, I.C.C., *EDI TERMS Project - Call for Participation in Working Party*, Working Party on EDI, Doc. No. 460-10/Int. 61 (Feb. 2, 1993). *But see* S.W.I.F.T., *ICC Proposal to Develop 'EDITERMS'*, Int'l Chamber of Commerce, Working Party on EDI, Doc. No. 460-10/8 (Oct. 1, 1993) (urging abeyance of the EDITERMS project due to "considerable opposition to the idea from certain quarters").

## **E. AGGRESSIVELY PROMOTE A RATIONALIZATION OF THE GLOBAL CERTIFICATE INFRASTRUCTURE**

While exercising caution to remain within the permissible bounds of federal practice and jurisdiction, it is critical that the federal government take a supportive role in assuring the development of a global public key infrastructure for its benefit and for that of business entities and U.S. citizens. The growing variation in approaches to policy and legal issues demonstrated by the European Commission's *Green Book*<sup>1317</sup> foreshadows such an approach. This rationalization should address technical standards and performance criteria, as well as relevant policy and legal issues. The task should not be left exclusively in the hands of private and international standards-making entities because, in part, such entities lack the necessary expertise and influence or otherwise do not share the desire to promote the legitimate interests of the federal government.

## **F. ORGANIZATIONAL STRUCTURE**

The FCA's organizational structure and situs (*e.g.*, an agency of the Executive Branch; an independent government-sponsored entity such as the USPS; or a private government contractor), should be selected to assure independence (both actual and apparent); disinterestedness (again, both actual and apparent); and, at least in experimental implementations, very limited liability. Independence and disinterestedness would likely best be enhanced by placing (part of the most critical-trusted portions of) the FCA in a *public* entity protected from Executive Branch interference.

---

<sup>1317</sup> See *supra* text accompanying note 28.



#### **G. DEVELOP AN APPROPRIATE INTERFACE BETWEEN THE FCA, OTHER FEDERAL ORGANIZATIONS AND PRIVATE THIRD PARTY SERVICE PROVIDERS, INCLUDING NON-FCA CERTIFICATION HIERARCHIES**

The FCA will need to communicate with and rely upon diverse federal organizations and commercial parties to support a viable infrastructure, whether or not its functions include certification of government contractors. Recognizing the problems and successes of TPSP interconnect agreements, and the disparities in commercial and governmental liability and regulation, the FCA should formally develop mechanisms to ensure the flexible and productive cooperation and interface between the private and public sectors. This will require considerable consultation and cooperation among the FCA and the many regulatory bodies mentioned herein.

#### **H. DEVELOP SPECIAL PRESUMPTIONS FOR FCA-ENHANCED COMMUNICATIONS**

To the extent that the use of FCA services will presumably provide users with greater assurances of certainty, security, non-repudiation and legal enforceability than are available with non-FCA-enhanced communications, FCA users can expect to derive discernible benefits from the FCA. One such benefit might take the form of a relaxation of the quantum of evidence required to prove the adequacy and integrity of the digital signature of FCA-issued certificate holders. It should be noted that the FCA's powers of enforcement (with respect to users), absent specific legislation, would likely be limited to issuing CRLs, suing for breach of contract and seeking criminal prosecution. In other words, there is a comparative lack of control that contrasts sharply with military or classified security control over matters within their respective jurisdictions.

#### **I. DEVELOP AN FCA INFRASTRUCTURE THAT LIMITS, RATHER THAN EXCLUDES, LIABILITY**

The extent of FCA liability will depend upon how FCA services are characterized and should be based on an appropriate balancing of competing government and private interests that reflects both the need to make the FCA economically viable (tending to limit liability) *and* the need to provide reasonable compensation to persons injured as a result of the FCA's actions (tending to expand liability). Consequently, it is recommended that the FCA should permit itself to be sued, but that reasonable limitations be placed on liability.

#### **J. DEVELOP AN FCA INFRASTRUCTURE THAT PROVIDES FLEXIBLE LIABILITY LIMITS**

Given the diverse uses that the FCA will support, as well as the extent of potential risks, PCAs should, in a rational and comprehensive manner, offer different levels of indemnification, insurance and/or liability limitations. As an alternative or as a supplement to the foregoing, users should be able to tailor the extent of protection to their requirements, for a price. That is, each PCA might offer different "levels of service" and charge corresponding different prices accordingly.

#### **K. UTILIZE CARD TECHNOLOGIES IN EARLY PILOTS**

Given the level of confusion, the lack of business practice and laws, and the lack of diverse alternatives to ensure sufficient binding associated with card technologies, there is significant need to experiment with and to assess the viability of card technologies. The cost and reliability of cards requires explicit analysis and authoritative treatment and should explicitly compare attributes of both card technologies and software-based solutions. Experimentation with, and implementation of, card technologies should be incorporated into early FCA piloting.

#### **L. IDENTIFY AND IMPLEMENT REQUISITE AND APPROPRIATE DISCLOSURE, NOTIFICATION AND WARNING MECHANISMS**

The sufficiency of disclosures, notices and warnings to and among certificate-based public key cryptography users, particularly within a government context, requires resolution. Issues that require rationalization include the choice of media for giving notice (possibilities include the Federal Register and specific agreements) and whether that media will take paper or electronic form. Government policy, as exemplified by the different approaches taken by various federal agencies, remains unclear. Questions about potential consumer usage of the FCA exacerbate the uncertainty. Explicit, comprehensive, and authoritative rules are needed.



## **M. EVALUATE INSURANCE PARADIGMS**

Federal insurance programs should be carefully evaluated to determine whether they offer useful approaches to the apportionment of liability. The potential role and scope of private insurance also require analysis and should be contemplated in the development of the FCA infrastructure. Additionally, to facilitate flexibility and user decision-making respecting risk, message labeling and voluntary message-specific insurance should be examined (such as is available for USPS postal matter).

## **N. EVALUATE AND REFORM COMPUTER CRIME LAWS**

Due to (i) the complexity of certificate-based public key cryptography, (ii) the scope of issues it raises in the context of an FCA infrastructure, (iii) the focus of existing computer abuse and crime laws on *access* rather than on *authentication and integrity*, and (iv) the fact that legislators not have contemplated the nature of public key applications in the development of computer abuse and crime laws, there is a need for rigorous consideration of the strength and weaknesses of those laws, and recommendations concerning whether there is a need for legislative reform.

## **O. ASSURE THE ACCOUNTABILITY OF EMPLOYEES IN POSITIONS OF TRUST**

Rules that assure the trustworthiness of FCA employees, and consistent, swift and certain government-wide assurances of punishment for breach of fiduciary obligations, should be evaluated, articulated and implemented during the early pilot stage. Inconsistent or insufficient standards of conduct, and inadequate criminal sanctions (affecting both government and citizens), require review and corrective action.

## **P. INTEGRATE LEGAL RISK ANALYSIS INTO FCA RISK ANALYSIS**

Risk analysis for computer-based mechanisms, including electronic commerce, has not generally included a formal legal risk analysis on par with technical and security risk analysis. Because the FCA is contemplated to support diverse types of transactions, risk analysis should henceforth take an interdisciplinary approach.<sup>1318</sup> It should be recognized, however, that precise identification and quantification of risk will, to a considerable extent, require a trial period to see what forms legal concerns and relief will take.

## **Q. PROMOTE AND INTEGRATE AUDIT, LEGAL AND SECURITY EDUCATION EXTENSIVELY**

A sobering, if not alarming, fact that came to light during the research and interview phase of developing this Report was the almost universal ignorance of even basic concepts of legal or technical requirements for certificate-based public key on the part of both government and private executives at all organizational levels. Additionally, concern has been expressed that a viable FCA must wait until a more computer-literate generation becomes the mainstream in society. Consequently, it is recommended that the government expeditiously develop, promote and perhaps require participation of all FCA participants in a comprehensive training program that will include the audit, legal, administrative, and, of course, technical issues and solutions required for a successful FCA implementation. This program should include hands-on workshops to assist in the development of appropriate policy, regulation and guidelines. The government should also develop plans to integrate information security into academic courses and course requirements.

## **R. RESEARCH THE IMPLICATIONS FOR CONSUMER USE OF THE FCA**

The legal implications for consumer use of the FCA require rigorous study because consumers will ultimately require or demand FCA services. The issues

---

<sup>1318</sup> The Carnegie Commission has noted that "the federal government is not effectively equipped to determine which risks are 'worst' or to coherently and efficiently respond to them." It "recommends the creation of a high-level, interagency Regulatory Coordinating Committee comprised of risk reduction agencies and of the Executive Office to meet this need. . . . the agencies should develop methods for integrating informed societal values into relative risk analysis . . . [and] the creation of more opportunities for informal but structured interbranch communication." Carnegie Commission, *Carnegie Commission Report Calls for Strengthening of Federal Risk-Based Regulatory Decision Making*, Press Release (Wash., D.C., June 30, 1993).



arising from the Treasury's Electronic Benefit Transfer initiatives exemplify the potential complexity associated with implementing new cryptographic technologies in the consumer context. Also, because consumer needs will inevitably require accommodation, planning for the inclusion of consumer requirements should begin now.

#### **S. DEVELOP (OR BOLSTER) A MULTIDISCIPLINARY FCA DEVELOPMENT GROUP**

In addition to the current technical and administrative coordinating group(s) composed of participating and interested government agencies, a viable and extensible FCA demands the early development of (or formal inclusion in an existing) a public advisory or related group to provide advice and respecting private sector requirements to facilitate domestic (both regionally and nationally), international and consumer needs. This group should also contribute to pilot synchronization, legislative initiatives, policies and technical analysis. Finally, this group can be a magnet to ensure that groups such as the banking, credit card, computer and telecommunication industries provide input (perhaps including the use of focus groups) and ultimately promote the FCA.

#### **T. PROMOTE AND PARTICIPATE IN ATTRIBUTE CERTIFICATE METHODOLOGIES**

Attribute certificate models, such as those currently under development in ANSI X9.F1, provide promising contributions to improved security and liability management, in the areas of authorization, delegation, restriction, time stamping, level of service and accreditation. Attribute certificate models should be carefully evaluated to determine the extent to which they should be accommodated by the FCA.

#### **U. RECOMMENDATIONS FOR FURTHER WORK**

Each of the above recommendations requires further analysis and development to test their validity, and to ensure their viability and successful implementation.

\*\*\*

## **XI. APPENDICES**

### **APPENDIX A - LINKING SECURITY**

The paper *Linking Security* begins on the next page.



**Workshop on Security Procedures for the  
Interchange of Electronic Documents**

**National Institute of Standards and Technology  
Gaithersburg, Maryland  
November 12-13, 1992**

**Abridged Version**

**LINKING SECURITY AND  
THE LAW OF COMPUTER-BASED COMMERCE**

**by**

**Michael S. Baum, J.D., M.B.A.  
Independent Monitoring  
Cambridge, Massachusetts USA**

**© 1992, 1993 Michael S. Baum All Rights Reserved**

## PREFACE

It is frequently (and astutely) stated that the law has not kept pace with technology. The historical tensions of law reform intended to accommodate technological change are manifested in the words of Oliver Wendell Holmes, who said

[a]s few could write, most people had to authenticate a document in some other way, for instance, by making their mark. This was, in fact, the universal practice in England until the introduction of Norman customs. With them seals came in. But as late as Henry II they were said by the Chief Justice of England to belong only to kings and to very great men. I know no ground for thinking that an authentic charter had any less effect at that time when not under seal than when it was sealed. . . . Its conclusive effect was due to the satisfactory nature of the evidence, not to the seal. . . . But when seals came into use they obviously made the evidence of the charter better, in so far as the seal was more difficult to forge than a stroke of the pen.<sup>1</sup>

Similarly, the Supreme Court stated that

[f]ormerly wax was the most convenient, and the only material used to receive and retain the impression of a seal. . . . We cannot perceive why paper, if it have that capacity, would not as well be included in the category. The simple and powerful machine, now used to impress public seals, does not require any soft or adhesive substance to receive or retain their impression. The impression made by such a power on paper is as well defined, as durable, and less likely to be destroyed or defaced by vermin, accident, or intention than that made on wax. It is the seal which authenticates, and not the substance on which it is impressed; and where the court can recognize its identity, they should not be called upon to analyze the material which exhibits it.<sup>2</sup>

Just as prior generations have grappled with document trustworthiness, today we must creatively forge a path which accommodates current requirements and practices, while contemplating the future. *Solutions* necessarily require compromises -- the challenge is to develop solutions and compromises that are thoughtful, practical and extensible. This is a daunting undertaking, but it is, at the same time, necessary and exciting.

---

<sup>1</sup> OLIVER WENDELL HOLMES, *THE COMMON LAW* 272-273 (1881).

<sup>2</sup> *Pillow v. Roberts*, 54 U.S. (13 How.) 472, 473-74 (1851).



# TABLE OF CONTENTS

<b>I. Introduction .....</b>	
<b>II. Security and Reliability .....</b>	
<b>a. Treatment in the Law.....</b>	
<b>b. Reasonable Security Procedures .....</b>	
<b>c. Mapping Security Attributes to Legal Standards.....</b>	
<b>Table 1 - Comparison of Signed Writings and Electronic Information* .....</b>	
<b>Table 2 - Fallibilities of Paper-based Signatures.....</b>	
<b>d. Non-repudiation .....</b>	
<b>e. Trusted Entities and Time Stamping .....</b>	
<b>III. Risk Analysis and Risk-Based Approaches .....</b>	
<b>a. Risk Analysis.....</b>	
<b>b. Security Baseline Issues.....</b>	
<b>Table 3 - Relative Levels of Abstraction.....</b>	
<b>Table 4 - Survey of Costs in Implementing Cryptography .....</b>	
<b>Table 5 - Primary Beneficiary of Security .....</b>	
<b>c. A Model Security Baseline .....</b>	
<b>IV. Burden of Proof and Presumptions .....</b>	
<b>Table 6 - Substitute Model Baseline Section 3 - Legal effect.....</b>	
<b>V. Integrating Formalistic &amp; Evidentiary Requirements.....</b>	
<b>Figure 1 - A Hypothetical Cradle-to-Grave Transaction.....</b>	
<b>Table 7 - Effect of Differing Formalistic &amp; Foundational Requirements .....</b>	
<b>VI. Conclusion.....</b>	
<b>Appendix - The Model Security Baseline Graphics.....</b>	

## ACKNOWLEDGMENTS

The author gratefully acknowledges the comments and suggestions of many people, and particularly the significant comments and suggestions of the following people: Thomas Armstrong, Esq., U.S. General Accounting Office; George Chandler, Esq., Hill, Rivkin, Lomberg, O'Brien, Mulroy & Hayden; Douglas S. Cohen, Boston University Law School; Jerry Cohen, Esq., Perkins, Smith & Cohen; Clyde Christofferson, Esq.; Richard Dodd, Esq.; Sandy Epstein, Racal-Guardata, Inc.; Robert Fougner, Esq., PKP; Françoise Gilbert, Esq.; Altheimer & Gray; Gregory A. Gilbert, Boston University Law School; Ted Humphreys, XISEC Consultants Ltd.; Claire Johnson, Esq., Wilde Sapte; Gregory P. Joseph, Esq., Fried, Frank, *et al.*; Steve Kent, Ph.D., BBN; Professor Emeritus Alfred I. Maleson, Suffolk University Law School; Jerry Rainville, Esq., NSA; Miles Smid, NIST; Thomas Smedinghoff, Esq., McBride, Baker & Coles; Lee Stanton, General Electric Information Services; Oliver Smoot, Esq., CBEMA; and Peter Weiss, Esq., OMB.

## AUTHORSHIP

Michael S. Baum is Principal of Independent Monitoring, a Cambridge, Massachusetts consultancy specializing in electronic data interchange and electronic commerce law and security. Baum chairs the EDI and Information Technology Division and the Information Security Committee, Section of Science and Technology, American Bar Association. The views expressed in this article do not necessarily reflect those of any organization or person other than the author. Because this paper presents some new or otherwise untested ideas, and because the subject matter of this paper begs further debate and consideration, comments and criticism are respectfully solicited.

Michael S. Baum  
33 Tremont Street  
Cambridge, MA 02139-1227 USA  
FON: 1-617-661-1234  
FAX: 1-617-661-0716  
INTERNET: baum@hulaw1.harvard.edu



# LINKING SECURITY AND THE LAW OF COMPUTER-BASED COMMERCE

by

Michael S. Baum, J.D., M.B.A.

## I. INTRODUCTION

The accelerating movement from paper-based transactions and records to their electronic replacements, and the resulting benefits from this movement, are well documented. Yet in many cases, the shift from conventional to electronic mechanisms has not enjoyed sufficient legal consideration and treatment. Real and *perceived*<sup>1</sup> security weaknesses of electronic transactions and records remain legal and practical barriers to their effective widespread use. This paper considers the legal efficacy<sup>2</sup> and expanded use of electronic transactions and records in modern commerce, government, and other environments for undertaking commitments and other important purposes. The paper also asserts that information security mechanisms exist, considers their associated costs and benefits, and advocates, where appropriate, the use of such mechanisms. A model security baseline is proposed. The goal is to arrive at a reasonable level of security for various classes of transactions and records to provide assurances of satisfying legal requirements. The thrust of this paper, however, focuses on the legal implications of authentication, integrity, non-repudiation and availability rather than on those of confidentiality. This focus is not intended, however, to underplay the criticality of responsive private and government treatment of confidentiality issues – indeed, confidentiality is the most critical requirement in some applications.<sup>3</sup> While this paper presents some "action-oriented" proposals, clearly the work has only begun.

---

<sup>1</sup> Arguably, perceived security weaknesses could be reduced or eliminated by accepting commercially reasonable security practices (*see infra*). The failure to do so causes perceived weaknesses to become unnecessary barriers.

<sup>2</sup> *Legal efficacy* in this paper denotes wide legislative and judicial recognition that properly secured electronic transactions and records satisfy traditional legal indicia of reliability. These indicia include, where appropriate, transactions or communications considered to be *in writing*, *signed*, *verified*, or *acknowledged*. Such legal requirements often differ considerably among states and among nations, as well as by application.

This paper neither endorses nor condemns *writing*, *signing*, or other requirements that historically support conventional paper-based attestations and commitments. Legal analysis of these requirements and responsive private and legislative reform should consider and reflect pragmatically the underlying attributes and objectives of such requirements (*e.g.*, authentication and integrity). A mere redefinition of *writing* and *signature* is not recommended.

<sup>3</sup> *See, e.g.*, WORKGROUP FOR ELECTRONIC DATA INTERCHANGE (WEDI), REPORT TO SECRETARY OF U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, Recommendation 8 (relating to confidentiality – the WEDI recommendations did not include a comparable recommendation on information authenticity and integrity) (July 1992).

## II. SECURITY AND RELIABILITY

### a. Treatment in the Law

The creation, processing, communication, control, management, storage, use, retention, and retrieval of information in electronic form<sup>4</sup> have become critical to modern society. However, Electronic Data Interchange ("EDI") and transactions and records in electronic form are not yet accorded the extent of the legal efficacy enjoyed by paper-based transactions and records. Before these electronic forms can earn this legal efficacy, they must establish customs and practices, or they must at least be judged legally equivalent to their manual counterparts.<sup>5</sup> This problem of legal efficacy arises in the following areas of law, among others: contracts, evidence, government procurement and regulation, criminal law, real property, and the judicial process.

1. Contracts -- Seeking to satisfy requirements for electronic transactions and records under the Uniform Commercial Code ("U.C.C."), raises certain fundamental issues.<sup>6</sup> For example, although the definition of *signed* in U.C.C. § 1-201(39) "includes any symbol executed or adopted by a party with the present intention to *authenticate* a writing" (emphasis added), the word *authenticate* is not defined in U.C.C. Articles 1 or 2 (although Official Comment 39 to U.C.C. § 1-201 includes mention of a thumbprint (a particularly forensically-intensive<sup>7</sup> type of authentication). This lack of definition has created confusion in the legal community. While the case law considering electronic writings and signatures is sparse and inconsistent, some of those cases addressing the issue confirm the importance of the probative value of signatures.<sup>8</sup>

---

4 Hereinafter, references to *records* or *information in electronic form* will include their electronic creation, processing, communication, control, management, storage, use, retention and retrieval unless expressly qualified.

5 EDI technical and security standards do not serve as a substitute for responsive legal consideration. Such standards are purposefully drafted to provide options and alternatives to accommodate use by diverse industries and do not necessarily provide the guidance necessary to assure the creation of unequivocal legal acts. Technical standards developers cannot properly analyze and resolve complex legal issues.

6 See, e.g., U.C.C. § 2-201 (Statute of Frauds); U.C.C. § 1-201(39) (defining "signed") and U.C.C. § 5-104 (addressing Formal Requirements and Signing).

7 See generally, BAUM, EDI AND THE LAW (Walden, ed. 1989) § 9.4 "The signing Requirement" at 123-125 (asserting that signatures and their electronic analogs should carry "forensic characteristics providing probative evidence of identity").

8 See *In re Carlstrom*, 3 U.C.C. Rep.Serv. 766, 773 (Bankr. D.Me. 1966) (requiring the affixed symbol for signature purposes under U.C.C. § 9-402 (Formal Requisites of Financing) to be *susceptible of evidentiary connection to the signatory*).



2. Evidence -- The Federal Rules of Evidence do not address specifically electronic digital data security mechanisms.<sup>9</sup> The scope of proof of trustworthiness (and, arguably, security) as an evidentiary foundation requires closer scrutiny. "[B]ecause electronic files are particularly susceptible to purposeful or accidental alteration, or incorrect processing, laying a foundation for their admission must be done with particular care. Proper control over creation and maintenance of these files can be crucial in overcoming inevitable objections that will be raised in the courtroom."<sup>10</sup> The implications of burgeoning, open, interconnected, and highly diverse computer systems utilizing expert system components, which may change frequently and considerably, may call for strong evidentiary foundations.<sup>11</sup>

There is some case law supporting the notion that proof of reliability (and implicitly security) is recognized as appropriate and necessary in evaluating the admissibility of computer-based evidence.<sup>12</sup> Other cases suggest a relaxation of the foundation required for admissibility of certain computer-based information (absent abuse of discretion by the judge).<sup>13</sup>

The Manual for Complex Litigation Second (1985) recognizes and addresses this problem of proof of reliability, yet by focusing on weight rather than admissibility, it reaches an equivocal, and ultimately unsatisfactory, solution of such evidentiary issues. It observes that "[n]otwithstanding the capacity of computers to make tabulations and calculations involving enormous quantities of information . . . several sources of potential errors of great magnitude exist."<sup>14</sup> The Manual further notes that the proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy,<sup>15</sup> and "the existence or possibility of errors usually affects only the weight, not the admissibility of the evidence, except when the problems are so significant as to call for exclusion . . ."<sup>16</sup>

---

<sup>9</sup> Cf. FED. R. EVID. 901(b)(9) (Process or system), 1001(1) (Writings and recordings), 1001(3) (Original), 902 (Self-Authentication), and N.J. R. EVID. 1(13) (writing); see Peritz, *Computer Data and Reliability*, 80 Nw. U.L. Rev. 956 (1986) reprinted in 7 Comp. L.J. 23 (1986).

<sup>10</sup> U.S. DEPT. OF JUSTICE, *ADMISSIBILITY OF ELECTRONICALLY FILED FEDERAL RECORDS AS EVIDENCE: A GUIDELINE FOR FEDERAL MANAGERS AND COUNSEL* (Oct. 1990) at 2.

<sup>11</sup> See Section V. INTEGRATING FORMALISTIC AND EVIDENTIARY REQUIREMENTS, *infra* (examining evidentiary requirements for the laying of a foundation).

<sup>12</sup> See *U.S. v. Scholle*, 553 F.2d 1109, 1124-25 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977) (stating that computer storage needs a more comprehensive foundation for admissibility, including testimony on procedures for input control, such as a test for insuring accuracy and reliability).

<sup>13</sup> See, e.g., *Rosenburg v. Collins*, 624 F.2d 659 (5th Cir. 1980); *U.S. v. Vela*, 673 F.2d 86, *reh'g den.* 677 F.2d 113 (5th Cir. 1982), and *U.S. v. Linn*, 880 F.2d 209 (9th Cir. 1989). Note, however, that each of these cases involved telephone company billing records -- records which are created and retained by trusted third parties.

<sup>14</sup> *MANUAL FOR COMPLEX LITIGATION SECOND* § 21.446 (1985).

<sup>15</sup> *Id.*

<sup>16</sup> "In view of the complex nature of the operation of computers and general lay unfamiliarity with their operation, courts have been cautioned to take special care to be certain that the foundation is sufficient to warrant a finding of trustworthiness and that the opposing party has full opportunity to

3. Government Procurement and Regulation – Interpretation and resolution of State, Federal and foreign requirements such as those concerning signature requirements remains unsettled. Compare the following varied – arguably conflicting – signature definitions.

- i. *signature* - "includes a mark when the person making the same intended it as such"<sup>17</sup>;
- ii. *signed* - "includes any symbol executed or adopted by a party with the present intention to authenticate a writing"<sup>18</sup>;
- iii. *signed* - "shall include the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols executed, adopted or authorized as a signature"<sup>19</sup>;
- iv. *signature* - "in the case of an EDI transmission, means a discrete authenticating code intended to bind parties to the terms and conditions of a contract"<sup>20</sup>; and
- v. *electronic signatures* - "characters representing the nominated persons on documents, and signed or symbols identifying their writers."<sup>21</sup>

One working group which considered this issue apprehended the effect of such uncertainty when it concluded that "[t]he lack of adoption of an accepted electronic signature policy by the [Department of Defense] will prevent some contract transactions being conducted in digital form."<sup>22</sup> Independently, the Comptroller General has addressed uncertainty in electronic commerce with the following decision: "[c]ontracts formed using Electronic Data Interchange technologies may constitute valid obligations of the government for purposes of 31 U.S.C. § 1501, so long as the technology used provides the same degree of assurance and certainty as traditional 'paper and ink' methods of contract formation."<sup>23</sup> Nevertheless, outside of the specific circumstances presented in the NIST case, the decision begs for a closer definition of the indicia of assurance and certainty necessary to be deemed reliable.

---

inquire into the process by which information is fed into the computer." MCCORMICK, HANDBOOK OF THE LAW OF EVIDENCE, (2d Ed. 1972) at 734.

<sup>17</sup> 1 U.S.C. § 1.

<sup>18</sup> U.C.C. § 1-201(39).

<sup>19</sup> 17 C.F.R. § 230 (1990).

<sup>20</sup> 41 C.F.R. § 101-41.002(d) (1990).

<sup>21</sup> Korean Act on Promotion of Trade Business Automation (1992) (Law No. 4479 Enacted Dec. 31, 1991) Art. 2.8 (Definitions, "Electronic Signature") reprinted in UN/ECE/TRADE/WP.4/R.872 (Aug. 4, 1992) (hereinafter "Korean Act") at 5.

<sup>22</sup> Legal Issues Committee of the Acquisition Task Group, CALS/EC Industry Steering Group, Report on Potential Legal Issues Arising from the Implementation of CALS (Nov. 10, 1991) at 10.

<sup>23</sup> Matter of National Institute of Standards and Technology—Use of Electronic Data Interchange Technology to Create Valid Obligations, Dec. of the Comp. Gen. of the U.S., File B-245714 (Dec. 13, 1991). See TABLE 2 - FALLIBILITIES OF PAPER-BASED SIGNATURES, *infra* Section.II.c.



4. Real Property – An example of how the problem of legal efficacy of electronic information could arise in the real property area involves the recording of deeds and related instruments where the recording statute mandates that "writings which are to be recorded or docketed in the clerk's office of courts of record in this Commonwealth shall be an original or first generation printed form, or legible copy thereof, pen and ink or typed ribbon copy. . . ." <sup>24</sup> Such a statute raises considerable barriers to computer-based commerce.
5. In Relation to the Judicial Processes -- The legal efficacy of information in electronic form also arises in judicial contexts. Despite the advance of computer automation in some aspects of the judicial process, electronic notice and service of process are not generally permitted by court rules. However, there are exceptions, <sup>25</sup> and judicial reform is accelerating. <sup>26</sup>

It is evident from the above discussion of the different legal fields that there is need for legal reform. As noted in the *Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission* ("UNCID"), a pioneering international code of conduct that addresses important legal and control considerations attendant to the use of electronic trade data, the

electronic document is quite different [from a paper document]. It takes the form of a magnetic medium whose data content can be changed at any time. Changes or additions will not appear as such . . . it is possible to establish techniques which give electronic data interchange characteristics that make it equal or superior to paper not only as [a] carrier of information, but also as regards the evidential functions. <sup>27</sup>

Moreover, electronic transactions are increasingly communicated within open, distributed and interconnected environments. <sup>28</sup> These environments potentially expose users and networks to risks from both accidental and deliberate alteration and destruction of data, <sup>29</sup> because open environments are generally more

---

<sup>24</sup> VA. CODE § 55-108.

<sup>25</sup> E.g., FED. R. APP. P. 25(a) (1991) (authorizing a court of appeals to accept papers filed "by facsimile or other electronic means"); OHIO R. C. P. Rules 5(e) and 10 (July 1, 1991). The National Archive and Records Administration's *Electronic Records Management* regulations accommodate the judicial use of electronic records pursuant to FED. R. EVID. 803(8). 36 C.F.R. § 1234.24 (1990).

<sup>26</sup> Additionally, the U.S. Department of Justice has issued findings which "encourage the development of electronic data interchange technologies." BUREAU OF JUSTICE STATISTICS, REPORT OF THE NATIONAL TASK FORCE ON CRIMINAL HISTORY RECORD DISPOSITION REPORTING, NCJ-135836 (June 1992) at 1.

<sup>27</sup> INTERNATIONAL CHAMBER OF COMMERCE, Pub. No. 452 (1988) at 8.

<sup>28</sup> See generally, NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK, SAFE COMPUTING IN THE INFORMATION AGE (1991) (hereafter "NRC").

<sup>29</sup> See Eckerson, *Network security lacking at major stock exchanges*, Network World (Sept. 16, 1991) at 23-24; Prefatory Note, U.C.C. Art. 4A (1990); see also *Shell Pipeline v. Coastal States Trading*, 788 S.W. 2d 837 (Tex. Ct. App. 1990) (Shell's responsibility for correction of errors was upheld, even where Shell's undertaking was "entirely gratuitous").

difficult to control than are closed ones.<sup>30</sup> "New vulnerabilities are emerging as computers become more common as components of domestic and international financial systems. *The nation needs computer technology that supports substantially increased safety, reliability, and, in particular, security.*"<sup>31</sup>

Additionally, in open environments, parties will increasingly desire or need to communicate and make commitments without having executed electronic trade and communication agreements. Consequently, the degree of *end-to-end* security<sup>32</sup> in such trading environments takes on increased importance.<sup>33</sup> "[I]f the information is shared between user groups or exchanged via a public or generally accessible [] network . . . [n]either the technology, terminals and services nor the related standards and procedures are generally available to provide comparable security for information systems in these cases."<sup>34</sup>

Although the extent (or strength) of the security necessary to support reliable electronic transactions and records for legal purposes is unclear, security is increasingly recognized as critical.<sup>35</sup> This conclusion is supported by decisions, studies and opinions of public and private entities. For example, the United Nations Commission on International Trade Law (UNCITRAL) stated that "it is clear that the legal reliability of EDI techniques requires that high standards be used to determine legal certainty as to the identity of the sender, its level of authorization and the integrity of the message."<sup>36</sup> The Comptroller General of the United States has remarked that "[a]gencies can create valid obligations using *properly secured* EDI systems."<sup>37</sup>

---

<sup>30</sup> Because conventional management techniques and controls cannot respond adequately to open and distributed environments, technology-based techniques and controls may be necessary.

<sup>31</sup> NRC, *supra* at 2 (emphasis by Council). This view is substantiated by reports of increasing problems. For example, "[i]t [was] estimated that security breaches, including lost revenue, data recovery, lost computing time, and personal downtime . . . cost U.S. corporations \$1 billion in 1990." YANKEE GROUP, DATA NETWORK RELIABILITY AND SECURITY (1990).

<sup>32</sup> End-to-end security refers to those sets of services that are applied to information prior to their submission to the communication mechanism. These services provide security assurances throughout the transfer to the intended recipient and which are verifiable by the recipient. Such services may include, but are not limited to, digital signatures for authenticity and integrity, and encryption for privacy purposes.

<sup>33</sup> The U.S. Department of Defense has recognized the weaknesses in such open communications environments: "[i]t is important to reiterate that the CN [communication network] is not relied upon for the confidentiality or integrity of the information it transfers. Failures in a CN can only result in the delay, mis-delivery, or non-delivery of otherwise adequately protected information." Draft DOD INFORMATION SYSTEMS SECURITY POLICY at § 4.4 "FIRST PROTECTION ALLOCATIONS" (March 30, 1992) (note: this is not yet DoD policy).

<sup>34</sup> E.C. *supra* at Annex, Action Line 3.1.

<sup>35</sup> E.C., *supra* Action Line 4.1. ("In the security of information systems there is inherently a very close relationship between regulatory, operational, administrative and technical aspects.").

<sup>36</sup> *Electronic Data Interchange*, Rep. of the Sec. Gen., UNCITRAL, 246th Session, Vienna, 10-28 June, 1991, U.N. Doc. A/CN.9/350 (15 May 1991) at 23.

<sup>37</sup> Dec. of the Comp. Gen., *supra* (emphasis added).



Other supporting opinions can be seen in model trade agreements and the developing literature. A model EDI agreement states that "[a]dequate security procedures are recognized. . . as critical to the efficacy of electronic communication. . . The use of adequate security enhances the reliability of those records and enhances the ability to prove the substantive terms of any underlying commercial transaction."<sup>38</sup> A further supporting view notes that "[l]egal reliability actually implies 'demonstrably and unarguably high standards of authorization, [sic] operational and access control and management' use of IACT [information and communication technology] systems. 'Authorisation,' further, implies 'accurate, precise and dependable identification, verification and authentication technologies and techniques which are, or may become, as legally acceptable as the conventional trust and comfort of a manual signature written in ink on paper.'"<sup>39</sup>

## **b. Reasonable Security Procedures**

Unlike conventional paper-based transactions and records, there is little jurisprudential guidance as to whether (and, if so, under what circumstances) a particular security technique, procedure or practice will provide the requisite assurance of reliability in electronic form. This lack of guidance concerning security is reflected in the multiplicity of current security and authentication practices within the EDI community. These practices, in many instances, appear to have been implemented in an *ad hoc* manner, with neither a clear understanding of the present state of law, nor the technical proof assurances of other chosen practices.<sup>40</sup> Where the law has responded, it has been arguably too vague -- such as a requirement to implement *reasonable security procedures*.<sup>41</sup>

While security procedures should certainly be reasonable, in certain situations a lack of specificity in defining "reasonable" security procedures may provide inadequate guidance causing such security procedures to fail in their intended purpose. . . . Specificity may help the parties implement and comply decisively and unambiguously with security procedures, reduce confusion and offer better expectations of reliability and certainty.

---

<sup>38</sup> A MODEL EDI TRADING PARTNER AGREEMENT § 1.4 Comment 1, *supra*.

<sup>39</sup> Stephen Castell, "The Legal Admissibility of Computer Generated Evidence Towards 'Legally Reliable' Information and Communications Technology (IACT)," COMP. LAW AND SEC. REP. (Jul.-Aug. 1989) at 7-8. (discussing the Appeal Study *Appendix on Evidence Admissible in Law* by S. Castell and the Central Computer and Telecommunication Agency, British Treasury, 1988; subsequently published as The Appeal Report, May, 1990).

<sup>40</sup> In a survey of EDI users, the mechanisms or procedures employed as legal signatures included the following: a "buyer code," a DUNS number and suffix, a password, a message authentication code, an account number, an ID/password combination, an "electronic verification of symbol and codes," and functional acknowledgments. LEGAL AND BUSINESS CONTROLS TASK GROUP, ACCREDITED STANDARDS COMMITTEE X12, 1990 SURVEY (1990).

<sup>41</sup> For example, in banking, a *security procedure* has been defined as: "a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." U.C.C. § 4A-201 "Security Procedure."



Security procedures should be sufficiently precise so that they are not subject to discretionary, self-serving interpretation, in part, because: (i) few standard security procedures exist in the law. . . . (ii) security technology is changing rapidly, and (iii) parties often hold particularly diverse opinions on appropriate solutions to security threats.<sup>42</sup>

One difficulty in developing responsive laws involves deciding the extent to which law should detail and endorse particular security techniques, procedures or practices.<sup>43</sup> Proponents of specificity argue that the electronic commerce community needs greater guidance<sup>44</sup> and that private agreements and legislation requiring only *reasonable security procedures* are vague and unworkable. Proponents of generality, on the other hand, argue that the endorsement of specific security procedures, practices or techniques leads to inflexibility and creates a presumption that the failure to implement such techniques, procedures and practices constitutes failure to exercise ordinary care. While recognizing these competing interests, a stronger viewpoint supports a measured movement toward greater specificity.

The electronic commerce community is asking lawyers to consider and to provide advice concerning signatures, security procedures and other related issues, but as yet, the legal community's experience with these issues is limited. Attorneys often defer to security professionals, who in turn seek the guidance of auditors, who then defer to attorneys. This *circle of deference* suggests that sufficiently concise answers to, responsibility for, and the resolution of, these issues are not quickly forthcoming. Moreover, it suggests that there is need for professional education in the system.<sup>45</sup> Further study is warranted in this area. Lawyers, security professionals and auditors should strive to provide education as a means to develop ideas on what attributes reasonable security would possess, as well as to identify responsive security services, their associated strengths, and when they can and should be implemented.

Consistent with this approach, the House of Delegates of the American Bar Association (ABA) has approved the first ABA Resolution that directly responds to critical legal-security issues affecting electronic data interchange and electronic commerce. The resolution requires the ABA to do the following:

---

<sup>42</sup> MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, § 7 Comment 5, (June, 1992), prepared by the EDI and Information Technology Division, Section of Science and Technology, American Bar Association, (hereinafter "MODEL AGREEMENT") 32 JURIMETRICS J. No. 4 at 601 *et seq.* (1992)); *see generally*, Michael S. Baum, *Commercially Reasonable Security: A Key to EDI Enforceability*, ACTIONLINE, (AIAG, Nov. 1989).

<sup>43</sup> Various legislation and guidelines mentions, or recognizes specific security technologies.

<sup>44</sup> "Buyers of cryptography cannot independently evaluate a seller's claims of product security." Sandy Epstein, "Striking a Balance: View on a National Cryptographic Policy," testimony before the National Computer System Security and Privacy Advisory Board, NIST (Gaithersburg, Sept. 1992).

<sup>45</sup> There are only a few formal law school course offerings applicable to computers and EDI legal issues and course offerings on information security legal issues are probably nonexistent. "A lack of EDI education is perhaps today's greatest hindrance to productive EDI usage and such implementation." Sokol, *EDI Education Pays Dividends*, Data Interchange (Dec. 1991) at 16.



[s]upport action by federal and state governments, international organizations, and private entities to:

a) facilitate and promote the orderly development of legal standards to encourage use of information in electronic form, including appropriate legal and professional education;

b) encourage the use of appropriate and properly implemented security techniques, procedures and practices to assure the authenticity and integrity of information in electronic form; and

c) recognize that information in electronic form, where appropriate, may be considered to satisfy legal requirements regarding a writing or signature to the same extent as information on paper or in other conventional forms *when appropriate security techniques, practices, and procedures have been adopted.*<sup>46</sup>

Consistent with the ABA approach, the United Nations Commission on International Trade Law ("UNCITRAL"), as early as 1985, recommended that governments "review legal requirements of a handwritten signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication."<sup>47</sup>

### c. Mapping Security Attributes to Legal Standards

There are various techniques available, with specified assurances to authenticate the source of, verify the content of, and control access to, data in electronic form. Many more of these techniques will develop as both the technology and the law evolve. History has demonstrated repeatedly that legal rules prescribing technology for authentication and related purposes have been a function of the available technology, historical accident or anomaly, and the technology's forensic<sup>48</sup> characteristics. It has also been transitory.<sup>49</sup>

The following table (TABLE 1) presents some of the attributes of conventional writing and signings as compared to their *approximate* electronic security analogs. The strength (and the propriety of the suggested analog) of any such security mechanism depends considerably on its implementation and the associated system controls. For example, in the case of a "signature" requirement, any appropriate

---

<sup>46</sup> Developed and submitted by the Section of Science and Technology to the House of Delegates of the ABA, the Resolution (no. 115) was approved on Aug. 19, 1992 (emphasis added).

<sup>47</sup> OFFICIAL RECORDS OF THE GENERAL ASSEMBLY, FORTIETH SESSION, SUPPLEMENT NO. 17 (A/40/17), ¶ 360.

<sup>48</sup> See generally, BAUM, EDI AND THE LAW, *supra* § 9.4 "The Signing Requirement" at 123-125 (asserting that signatures and their electronic analogs should carry "forensic characteristics providing probative evidence of identity").

<sup>49</sup> See Preface, *supra* (providing quotes that give insight into the forensic and transitory nature of technology-related rules).

security technique that provides comparable or superior attributes to those produced by the conventional use of a written signature should be satisfactory.<sup>50</sup> However, the various security attributes in TABLE 1 demonstrate that the handwritten signature does not have an unequivocal electronic analog.<sup>51</sup>

---

<sup>50</sup> Conventional paper-based handwritten signatures inherently have security attributes to the extent that, *e.g.*, ink cannot easily be erased without detection, paper is non-transient, and a signature is biometrically unique.

<sup>51</sup> These three examples of information in electronic form (categories "B," "C" and "D" in TABLE 1) are also used to support the security services provided in the Model Security Baseline in Section III.c., *infra*.



	A	B	C	D
*ATTRIBUTE*	CONVENTIONAL SIGNED WRITING COMMUNICATED VIA UNITED STATES POSTAL SERVICE	UNENCRYPTED INFORMATION WITH SYMBOL IN ELECTRONIC FORM COMMUNICATED VIA THIRD PARTY SERVICE PROVIDER	DIGITALLY SIGNED OR COSIGNED INFORMATION IN ELECTRONIC FORM <sup>52</sup> COMMUNICATED VIA THIRD PARTY SERVICE PROVIDER	DIGITALLY SIGNED & NOTARIZED INFORMATION IN ELECTRONIC FORM COMMUNICATED VIA THIRD PARTY SERVICE PROVIDER
Origin Authen.	Medium-Strong	Weak	Strong	Strong
Proof of Receipt	Return Receipt	Weak	Strong	Strong
Content Integrity	Partial	Weak	Strong	Strong
Time of Creation	Weak	Weak	Weak	Strong
Time of Dispatch	Postmark	Weak	Weak	Strong
Time of Receipt	Return Receipt	Weak	Weak	Strong
Time of Acknow.	Return Receipt	Weak	Weak	Strong
Singularity	Yes	No	No	Can be offered as a "registry" service
Biometric	Yes, signature	No, but available for resource access control	No, but available for resource access control and for cryptoignition <sup>53</sup>	No, but available for resource access control and for cryptoignition
Expression of Intent <sup>54</sup>	Indicia	Indicia	Indicia	Indicia
Non-repudiation	Partial	Weak	Strong, except time	Strong
Privacy	If enveloped <sup>55</sup>	Weak	Weak	Weak

**TABLE 1 - COMPARISON OF SIGNED WRITINGS AND ELECTRONIC INFORMATION\***

**Key to TABLE 1**

\* General Comment: Attributes exhibiting a propensity for forgery are listed as "Weak."

TABLE 1 includes subjective positions and is intended exclusively for pedagogical purposes.

A: A signed paper document sent by postal service.

B: Unencrypted (clear text) communicated via third party service provider (TPSP).

Satisfaction of many listed attributes depends largely on controls, including TPSP controls.

C: Digitally signed electronic document.

D: Digitally signed electronic document which is "notarized" (time stamped and digitally signed) by a trusted third party. In this Table, notarization is available (via *trusted box*) at the site of origin, at the respective TPSPs and at the site of receipt.

<sup>52</sup> While many security services are best implemented using digital signatures or comparable cryptographic methods, many can be implemented non-cryptographically, although not necessarily with comparable economy, strength, functionality or elegance.

<sup>53</sup> A quantity which enables a cryptographic algorithm(s) or device embodying a cryptographic algorithm(s) to operate which is generally implemented as a component of a secret quantity used to convert other quantities necessary for operation.

<sup>54</sup> This may vary among criminal and civil proceedings.

<sup>55</sup> "The Postal Service must preserve and protect the security of all mail in its custody from unauthorized opening, inspection, or reading of contents or covers, tampering, delay or other unauthorized acts." DOMESTIC MAIL MANUAL (DMM) § 115.1 "Importance of Mail Security;" "In general, no person may open, read, search, or divulge the contents of mail sealed against inspection . . ."

One additional comparison is instructive. A decision of the Comptroller General proffered three signature attributes as being necessary to create obligations which can be recorded against the government. TABLE 2 considers these attributes within the context of fallibilities of paper-based media.<sup>56</sup>

PROPOSED SIGNATURE ATTRIBUTES <sup>57</sup>	FALLIBILITIES
Unique to the Certifying Officer	Forgery. Where stamps and other mechanisms are used, the signature is not unique to the certifying officer.
Capable of Verification	Error prone. Signature comparison is an art as well as a science; verification often disregarded due to cost, ineffectiveness or unavailability.
Under Officer's Sole Control	Law permits other mechanisms which may not, without knowledge of custom and practice, provide assurances of sole control.
<i>Proposed effect:</i>	
Demonstration of Intent to be Bound <sup>58</sup>	Depends on the circumstances of its use. Not an inherent attribute.

TABLE 2 - FALLIBILITIES OF PAPER-BASED SIGNATURES

To the extent, *arguendo*, that the Comptroller General's decision is interpreted to substantially require the use of cryptographic methods<sup>59</sup>, three observations deserve consideration. First, despite an inference that paper-based signatures provide a good benchmark for authentication and provability, Table 2's proffered signature fallibilities effectively present a compelling case that supports the permissibility of non-cryptographically enhanced transactions where appropriate.<sup>60</sup> Second, the noted weaknesses of conventional signatures relative to digital signatures (*see* TABLE 1) support the legal efficacy of digital signatures in substitution for the latter. Third, although the decision does not expressly reference

<sup>56</sup> Cf., the quotes in the Preface to this paper concerning fallibilities of conventional media.

<sup>57</sup> Proposed by the Comptroller General of the United States.

Other signature attributes which have been proposed within the private and commercial sectors include attributes that: *identify* the signatory to the transaction; *demonstrate* that the signatory had the intent to formalize the information due to its importance; *create* a record acceptable to the dispute resolution mechanism; *evidence* the existence of a contract; and, *prevent* repudiation.

<sup>58</sup> This is not a formal attribute but instead a conclusion. Note also that some government representatives advocate that having established a signature, it is also necessary to demonstrate that the signature is *linked to the data*.

<sup>59</sup> Cryptography "embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use." ISO 7498-2-1988(E) § 3.3.20.

In further support of the appropriate use of technology-based solutions, *see* FINANCIAL MANAGEMENT SYSTEMS, OMB Circular No. A-127 (obliging government agencies to *use the most contemporary technology*); and T. J. Hooper, 60 F.2d 737 (1932) ("[a] whole calling may have unduly lagged in the adoption of new and available devices").

<sup>60</sup> *See infra* Section III.c. "A Model Security Baseline."



*non-repudiation*, it effectively focuses on the attributes of non-repudiation, thereby bolstering the utility of this comparatively unfamiliar service.

#### **d. Non-repudiation**

Some security services can provide diverse capabilities that are not necessarily provided by conventional paper-based techniques. One such security service is known as a *non-repudiation service*. Generally, non-repudiation services prevent a document's originator from denying the document's origin and provide *irrevocable proof of authenticity*.<sup>61</sup>

The Non-repudiation Service may be provided through the use of mechanisms such as digital signatures, encipherment, data integrity and notarization, with support from other system services such as Time Stamping and Security Services. The Non-repudiation Service can use a combination of these mechanisms and services as appropriate to satisfy the security requirements of the application in question. The goal of the service is to collect, maintain, make available and validate non-deniable proofs regarding data transfers between the originator and recipient.<sup>62</sup>

A non-repudiation service is presented as *one* example of a security service, which, whether or not cryptographically based, may satisfy requirements that are linked to conventional writings and signings, such as contributing to evidence of a party's intent to contract or to be bound. Although many existing legal requirements do not require absolute or non-repudiable proof, these security services offer the legal and control communities important tools and possibilities with which to fashion legal obligations to accommodate electronic practices (particularly the more important or risky obligations).

The time of the creation of a transaction or the submission of a transaction to an electronic messaging system, or the time when received or retransmitted by a third party service provider (TPSP), available to, received by, or acted upon by the intended recipient is critical in various applications. For example, where parties must file information electronically<sup>63</sup> (e.g., tax returns), or where an electronic bidding process closes at a time certain, or where the first to file a response wins<sup>64</sup>;

---

<sup>61</sup> MESSAGE HANDLING: EDI MESSAGING SERVICE, CCITT Draft Rec. F.435 (Version 5.0, June 15, 1990).

<sup>62</sup> ISO/IEC JTC1/SC21, Intro., WORKING DRAFT NON-REPUDIATION FRAMEWORK, N7082, Project 97.21.49.6 Q53 (July 1992).

<sup>63</sup> The definition of *filing* has come under review. [insert references and relation to receipt and model agreements.]. "The word *file* is derived from the Latin work 'filum,' and relates to an ancient practice of placing papers on a thread or wire for safe-keeping and ready reference. See MICHAEL S. BAUM AND HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW (Wiley, 1991) [hereinafter "Baum and Perritt"] at § 5.16 "UCC Security Interest Filings" (considering many electronic filing issues).

<sup>64</sup> See *Abourezk v. Federal Power Commission*, 513 F.2d 504, 505 (D.C. Cir. 1975) (where Judge Bazelon noted that "[d]ue to lack of synchronization between the clocks in the clerks' offices and those in the

trusted time stamping is recognized as a prerequisite to the proof of the completion of obligations of one party, and the transfer of obligations to another.

Despite the great benefits enuring from the use of digital signatures, they have some inherent limitations (as is true with any security mechanism) including an innate inability to provide "time-related" non-repudiation. Digital signatures and other cryptographic methods cannot, in the absence of a trusted entity, provide an unforgeable trusted time stamp. Therefore, to achieve *full* non-repudiation, time stamping must be undertaken by a disinterested party beyond the control of the parties to a transaction or record. Such a third party is a trusted entity.

#### e. Trusted Entities and Time Stamping

A trusted entity is an independent, unbiased entity capable of providing important security assurances that enhance the enforceability and reliability of electronic records. The key attributes of a trusted entity are that it is a *disinterested, unbiased, third party* trusted by the parties to the transaction and by the dispute resolution mechanism(s) relevant to a transaction or record. Simply stated, a trusted entity's administrative, legal, operational and technical infrastructure must be beyond reproach.<sup>65</sup>

A trusted entity can time and date stamp,<sup>66</sup> store (or forward) a "record copy" or hash of a transaction, keep an audited data log, or serve as an intermediary for other trust-based services between trading partners.<sup>67</sup> The trusted entity's record copy of an electronic transaction would control in the event of a dispute regarding a document's authenticity or timeliness.

The electronic notary<sup>68</sup> offers unique solutions to one of the critical "missing links" of electronic transactions and records assurances: unforgeable trusted time stamping. The electronic notary also may facilitate future TPSP and value added network service requirements by providing them with trusted-entity services.<sup>69</sup> The

---

offices of the various federal agencies, it is often not possible to be certain which petition was the first to be filed after the agency entered its order.").

<sup>65</sup> Third Party Service Providers or value added networks, such as ATT or MCI (collectively "VANs") have arguably been inaccurately identified as trusted entities. VANs are not necessarily disinterested because they may compete with each other, participate in the transfer or processing of information (and therefore have exposure), and may introduce error, delay, unavailability or misdelivery.

<sup>66</sup> The author offers a French term, which more concisely describes the intended time stamp functionality: *horodatage* (horo=hour, and datage=date). The use and significance of time stamping has both a rich historical as well as contemporary value.

<sup>67</sup> See BAUM AND PERRITT, *supra* at Ch. 5 (providing an extensive survey of possible trusted entity - clearinghouse services).

<sup>68</sup> The terms "notary" or "notarization" in the context of electronic transactions do not have recognized legal standing equivalent to that of the conventional notary public, and consequently, such terminology used in this setting is inaccurate or potentially confusing. See BAUM AND PERRITT, *supra* §§ 4.33-4.36 (presenting a survey of issues pertinent to the automation of the notary public).

<sup>69</sup> Because the electronic notary is not controlled by TPSPs or VANs, reliance by users need not be placed exclusively on the internal controls of the TPSPs and VANs, except for availability.



electronic notary can provide irrefutable proof of the time of the origination of the document.<sup>70</sup> Notarizing data intended for record retention and archiving provides an unforgeable seal which may contain a time stamp and digital signature, together with additional audit, legal and security information intended to enhance its legal efficacy.<sup>71</sup>

### III. RISK ANALYSIS AND RISK-BASED APPROACHES

#### a. Risk Analysis

To the extent that various methods to assure that reasonable security procedures have been considered and implemented in both the private and public sectors, results have been inconsistent -- just as attempts to satisfy amorphous requirements for *commercially reasonable security* have produced varying results.<sup>72</sup> Such inconsistent results are explained, in part, by the insufficient and varying analytical tools used to evaluate security requirements (and their legal efficacy), such as *risk analysis*.

'Risk analysis' is a procedure used to estimate potential losses that may result from system vulnerabilities and the damage from the occurrence of certain threats. Risk analysis identifies not only critical assets [and processes<sup>73</sup>] that must be protected but considers the environment in which these assets are stored and processed. The ultimate purpose of risk analysis is to help in the selection of cost-effective safeguards that will reduce risks to an acceptable level.<sup>74</sup>

The National Institute of Standards and Technology ("NIST") noted the need for EDI risk analysis in March 1991 when it required agencies to *employ risk management techniques*. Yet, NIST did not provide specific guidance on EDI risk

---

<sup>70</sup> Cf., the proofs available from an electronic notary to those available from the U.S.P.S.. For example, consider that "[m]ail deposited in a collection box or post office may, with proper identification, be recalled by the sender." DMM *supra* at § 152.71 "Who May Recall Mail."

<sup>71</sup> See *supra* (WORKING DRAFT NON-REPUDIATION FRAMEWORK).

<sup>72</sup> See *supra* Section II.b., Reasonable Security Procedures.

<sup>73</sup> See Thomas A. Stewart, "The Search for the Organization of Tomorrow," *Fortune*, (May 18, 1992) at 94-94 (includes a proposal for viewing the organization horizontally by core processes -- each core process is a set of functions necessary to meet a major external objective such as inventory turnover or on-time delivery).

<sup>74</sup> IRENE GILBERT, GUIDE FOR SELECTING AUTOMATED RISK ANALYSIS TOOLS, NIST Special Pub. 500-174 (1989) at 3. THE COMPUTER SECURITY ACT OF 1987, 40 U.S.C. § 759 note, P.L. 100-235 (1987), requires applicable federal agencies to develop a computer security and privacy plan "that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in" each Federal computer system.

analysis.<sup>75</sup> The creation and enforcement of legal commitments undertaken electronically may require new criteria (such as EDI-relevant legal criteria) and approaches to risk analysis that have either not been developed or widely adopted.<sup>76</sup> For example, EDI may involve variables and *higher order effects* that are difficult to quantify and that effectively require consideration of the legal interrelationship between a series of related EDI transactions and records without direct conventional analogs.<sup>77</sup> "EDI/EFT is too young for its full risk implications to become apparent."<sup>78</sup> There should be a move toward the development of authoritative risk analysis for electronic commerce in both the private and public sectors.

## **b. Security Baseline Issues**

In considering various approaches to linking technical security measures and the law, it is important to recognize that the strength and reasonableness of security procedures for particular applications are risk driven. These procedures, therefore, must undergo further scrutiny. A *security baseline*<sup>79</sup> ("baseline") is a tool that may help define and rationalize security requirements for diverse electronic transactions and records. A baseline serves as a foundation to develop a clear expression of security requirements, facilitate open trading environments, ensure that transaction costs are commensurate with the risks, and provide greater legal certainty.<sup>80</sup>

A baseline can encompass generally accepted security methods and procedures (to the extent available to attain reasonable security at the operating system, data communication, and application (including EDI) levels).<sup>81</sup> Compliance with such requirements would establish a presumption of the security procedure's sufficiency

---

<sup>75</sup> NIST, ELECTRONIC DATA INTERCHANGE (EDI), FIPS-PUB 161, 56 Fed. Reg. 13,123 (Mar. 29, 1991). Cf., NIST COMPUTER SYSTEMS LABORATORY (CSL) BULLETIN, SECURITY ISSUES IN THE USE OF EDI (June, 1991).

<sup>76</sup> Existing risk analysis tools focus neither on legal requirements nor on the particular needs of EDI. See NIST, GUIDELINE FOR AUTOMATED DATA PROCESSING RISK ANALYSIS, FIPS PUB 65 (Aug. 1979). Cf., Birch and McEvoy, "A Structured Approach to Information Security Risk," COMP. LAW & SEC. REP., Vol. 8 Issue 4 (Jul.-Aug. 1992) at 177.

<sup>77</sup> E.g., EDI Functional Acknowledgment and Application Advice transaction sets do not exist in conventional paper-based practices. The loss or garbling of such transaction sets present challenges to conventional risk analysis. See BAUM AND PERRITT, *supra* at 180-181.

<sup>78</sup> David Davies, "EDI Insurance - The 'Red Herring' Theory Examined," CLSR, Vol. 8, Issue 5 (Sept.-Oct. 1992) at 226-229 (noting "the relatively unproven or un-demonstrated nature of the risks;" and that "very little reliance should be placed upon the ability of existing insurances to encompass the new risks of EDI").

<sup>79</sup> See Baum, Actionline, *supra* at 35 (advocating a security baseline).

<sup>80</sup> The approach to the development of a baseline should be examined cautiously, considering that "[t]he law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics." OLIVER WENDELL HOLMES, THE COMMON LAW *supra*; and also taking into consideration that we should not take too formulaic an approach.

<sup>81</sup> See NRC, Recommendation 1 Promulgate Comprehensive Generally Accepted Security System Principles (GSSP) *supra* at 27-32.



or legal efficacy.<sup>82</sup> A Baseline can take various forms, including legislation, private agreement and guidelines.<sup>83</sup>

The purpose of a baseline is to serve as a bridge between high-level policy and philosophical positions on one end of the spectrum, and, at the other extreme, detailed application-specific rules. As such, a baseline is positioned at an intermediate level of abstraction which both seeks to enforce high-level policy and provides a mechanism for the development of workable rules. TABLE 3 provides one perspective on how a baseline can be used and where it fits into the legal-standards environment.

ABSTRACTNESS	TYPE	COMMENTS
High	"Reasonable Security Procedures"	Too uncertain for rules; Preferably a policy objective
Medium	Baseline (single or multilevel)	A tool to help enforce policy objectives
Low	Application-specific rules and guidelines	Compliant with Baseline

TABLE 3 - RELATIVE LEVELS OF ABSTRACTION

Baseline security requirements should vary depending on risks and on other factors.<sup>84</sup> For low risk transactions – *such as* those with a low probability of large losses, the benefits of strong security are likely outweighed by the costs of such measures.<sup>85</sup> Higher risk transactions may require more stringent controls, including cryptographic methods or trusted entity services.

A baseline should be sufficiently concise without regard to risk. The more specific the baseline, the greater will be the transactional certainty, user confidence, and ultimate success. Without specificity, security requirements may provide inadequate guidance and may fail in their intended purpose.<sup>86</sup> Specificity helps users to implement decisively and to comply unambiguously with baseline requirements. Consequently, until the parameters of *reasonable security* practices in electronic commerce become more clearly defined (as a function of improved experience and practice coupled with the use of better risk analysis tools), greater specificity is advocated. A baseline arguably fills this gap. Thereafter, generalized or abstract

---

<sup>82</sup> See *infra* Section IV. BURDEN OF PROOF AND PRESUMPTIONS (presenting an alternative to the legal effect of the Model Baseline in TABLE 6).

<sup>83</sup> See BAUM AND PERRITT, *supra* at 80-81 (discussing various forms of implementation guidelines).

<sup>84</sup> See the various factors described later in this section.

<sup>85</sup> For most electronically communicated commercial non-financial transactions, the security regime is typically little more than that provided by simple password/ID-based access or authentication controls. Such weak security probably results from established customs and practices, simplicity, lack of security sophistication, financial constraints, and the belief that password/ID-based access controls are the lowest common denominator (and, in this respect, are most pragmatic) for ubiquitous computer-based communications.

<sup>86</sup> See Michael S. Baum, *Commercially Reasonable Security: A Key to EDI Enforceability*, Actionline, *supra*; see also BAUM AND PERRITT, *supra* at 184.

standards of "reasonable security" may become legally sufficient -- in an environment benefiting from legal precedent, and widely recognized specific procedures and practices.<sup>87</sup>

In order to understand this idea, the following issues should be considered in developing a baseline (but not necessarily be limited to):

1. Attribute-based Security Requirements - The security of particular transaction types, and of a particular transaction, will depend upon the needed security services and will vary as a function of risk and legal needs. Security services include authentication, integrity, non-repudiation, confidentiality, and availability.<sup>88</sup> TABLE 1, *supra*, presents security attributes within the context of a comparison to paper-based mechanisms.
2. Value Requirements - Developing consensus on a definition of value<sup>89</sup> is becoming a focal point in the development of electronic commerce rules<sup>90</sup> in both the private<sup>91</sup> and public sectors<sup>92</sup>, and may go to the heart of the debate. The challenge is to determine which transactions, other than payment orders and "purely" financial transactions merit stronger information security protection (such as cryptographic-based authentication methods) than the security utilized for low value and low risk transactions. Two competing approaches on this issue are characterized as *narrow* and *broad*.

- Narrow View Argument - Based on value, transactions which merit stronger information security are comparatively few in number. Generally, the narrow view does not provide increased protection for

---

<sup>87</sup> Specific practices leading the way for acceptance of the general practice is analogous to traditional analysis in evidence law: initial close scrutiny of the trustworthiness of new technology prepares the way for future lenient acceptance of the new procedures -- coupled with a better understanding of the risks.

<sup>88</sup> See *supra* (providing definitions for each of these security services).

<sup>89</sup> Value may be defined broadly by the courts -- e.g., as "[a]ny consideration sufficient to support a simple contract." *Fowler v. Smith*, 156 N.E. 913, 914 (Ohio App. \_\_\_\_). Cf., U.C.C. § 1-201(44) (defining value broadly); U.C.C. § 2-714(2) ("Buyer's Damages for Breach in Regard to Accepted Goods);" and U.C.C. § 1-106 ("Remedies to Be Liberally Administered") (generally providing a subjective measure of damages; Official Comment 1 "rejects any doctrine that damages must be calculable with mathematical accuracy").

<sup>90</sup> This includes the development of a Model Security Baseline, see *infra* Section IIc.

<sup>91</sup> The National Automated Clearinghouse Association ("NACHA") does not distinguish between low and high value transactions where it "recommends that ACH [automated clearing house] processors and all ACH participants employ data security techniques in accordance with ANSI standards for authentication and key management." 1992 ACH Rules at OR xvii.

<sup>92</sup> Cf., "'Value' . . . will be determined on a case-by-case basis. In fact, Treasury itself moves very few funds. . . . The Treasury Directive on Electronic Funds and Securities Transfer Policy . . . makes it Treasury policy that *all* Federal EFT transactions be 'properly authenticated'. The authentication measures adopted . . . are those recommended by the American National Standards Institute (ANSI) in Standard X9.9." Treasury Directive 81-80, § 2.1.



purchase orders, "merely executory contracts,"<sup>93</sup> contract-related business documents (excluding payment orders) and other *low value*, low risk transactions. This view argues that business knows how to take care of itself, and business practices demonstrate that non-payment-related transactions are typically not communicated in a highly secured manner.<sup>94</sup> Business has determined that the cost of strongly securing purchase orders, invoices, and the like, is not commensurate with the risk.

•Broad View Argument - Individuals supporting this position believe that the scope of transactions of a value which merit stronger information security are comparatively broad. Many purchase orders, purchase order acceptances, and other non-payment documents require stronger security protection whenever the risk of loss or error associated with such documents threatens business assets or competitive position.<sup>95</sup> The value of a loss or error in a non-financial instrument may not necessarily result in as immediate a loss as with a financial instrument. However, the loss of, or litigation concerning, a non-financial instrument is nonetheless of comparable or greater value (such as where consequential damages are considered). Fiduciary duties owed by corporate management to its stock holders, include prudently protecting corporate assets -- and strong security is one prudent approach. Finally, paper-based practices demonstrate that the strength of security techniques implemented for low and medium value transactions do not vary considerably (except, *e.g.*, with respect to the use of multiple signatures for authorization), because low value transactions often are "bootstrapped" to a stronger security level.

A consideration of value-related issues properly includes: (i) how narrowly value should be defined;<sup>96</sup> (ii) whether value should be limited to *financial* value; (iii) if so, how broadly should *financial* be construed; (iv) how certain must value be (*e.g.*, how liquid; when should value be measured,<sup>97</sup> and should the potential value of consequential damages be included);<sup>98</sup> and (v) does the

---

<sup>93</sup> "That which is yet to be executed or performed; that which remains to be carried into operation or effect; incomplete; depending upon a future performance or event." BLACK'S LAW DICTIONARY 680 (4th ed.1968).

<sup>94</sup> Historically, cryptographic methods have (for other than national security purposes) largely only been required, or largely implemented, for financial purposes.

<sup>95</sup> Some advocates of the broad view argue that even this standard is too weak. Instead, they propose that any transactions of "commercial significance" or some other more encompassing standards should be used.

<sup>96</sup> Should the law focus on *clear value*, *face value*, *fair and equitable value*, *market value*, *true value*, or something else?

<sup>97</sup> In an action to recover chattel, "value" means value at time of trial, not at time of seizure thereof. *Spear v. Auto Dealers' Discount Corporation*, 278 N.Y.S. 561 ( ).

<sup>98</sup> Compare U.C.C. § 4A-305 ("Liability for Late or Improper Execution or Failure to Execute Payment Order") and U.C.C. § 2-715 ("Buyer's Incidental and Consequential Damages").

definition of *sensitive information* under the Computer Security Act of 1987 necessarily broaden the scope of value for such purposes?

A value limitation is ostensibly one of the most specific and well understood criteria. For example, statutes of frauds prescribe dollar limits, such as the \$500 threshold of U.C.C. § 2-201. Another example is the Federal Acquisition Regulations ("FARs") which provide for a \$25,000 threshold<sup>99</sup> and permit telephone bids/proposals or orders in an amount up to \$2,500.<sup>100</sup> Federal money laundering regulations require reporting if a \$10,000 daily aggregate amount is exceeded.<sup>101</sup> Specifying a baseline value has been criticized as both arbitrary and difficult to enforce; but, there are administrative rulings and interpretations that provide guidance and mitigate potential abuse of aggregate requirements.<sup>102</sup>

3. Costs of Implementation - Whether and how costs of security should impact baseline criteria are important issues to resolve. It is impossible to consider meaningfully the cost of resolving a problem until the nature of the problem and the underlying *requirements* are articulated. Premature consideration of costs may eliminate viable solutions; yet, intensive focus on cost (sometimes to the exclusion of all other factors) has been the linchpin for policy and legal reform efforts. The cost debate focuses on whether the use of cryptographic methods are a necessary component of "reasonable security procedures"<sup>103</sup> and whether the costs associated with cryptography are too burdensome to require.<sup>104</sup>

This "crypto cost debate" has two main camps. Proponents of wide-spread cryptography usage argue that (i) only cryptography can adequately protect against the threats in open systems and ubiquitous computing environments, and (ii) because the costs of cryptography will decrease with increased usage, cryptography is a viable, indispensable, and appropriate requirement. Opponents of wide-spread cryptography usage argue that (i) conventional paper-based practices are fallible and consequently computer-based practices

---

<sup>99</sup> 48 C.F.R. § 13 (Small Purchase and other Simplified Purchase Procedures) (1992).

<sup>100</sup> FAR 14.201-6(g)1 and 15.407(e)(1). The Defense FARs Supplement, 48 C.F.R. § 208.405-2 (allowing for oral procurement ordering from federal supply contractors).

<sup>101</sup> 31 C.F.R. § 103 (1990); 31 U.S.C. § 5315 (reports on foreign currency transactions).

<sup>102</sup> E.g., Administrative Rulings, Interpreting Treasury's Currency and Foreign Transactions Regulations, Fed. Reserve Reg. Serv. 88-1 (June 22, 1988).

<sup>103</sup> Although the debate is focused on cryptography, a substantial proportion of fraud is traceable to inadequate conventional controls. Superior conventional controls would largely protect against such fraud (excluding the open systems issues). In this respect, the costs associated with implementing proper management controls may dwarf the costs of cryptography.

<sup>104</sup> "When there is a homogeneous nationwide EFT network with standardized security techniques, it will become increasingly "cost effective" for criminal elements to develop the technology required to defraud the system, because this technology, once developed, could be applied nationwide against the cardholders of hundreds or even thousands of financial institutions." ANSI X9.9 Retail PIN Standard, § A.3. (Amer. Banker's Assn. 1982).



need not be any better,<sup>105</sup> and (ii) the costs of cryptography are greater than the costs associated with protecting conventional media.<sup>106</sup> Since this debate continues to obfuscate the rational development of policy and rules for computer-based media, cost issues deserve further examination.

Notwithstanding this debate, the commercial information security marketplace, and particularly the commercial cryptographic marketplace, are undergoing substantial changes which impact the accuracy of the cost analysis.<sup>107</sup> There is little rigorous publicly available analysis of the costs of implementing and using cryptographic methods.<sup>108</sup> A cost analysis for implementation of cryptography may include the additional costs, if any, incurred as a result of:

---

<sup>105</sup> This argument may fail to account for the new and improved tools, as well as the possibilities offered by modern technologies. *See supra* ABA Resolution § (a) in Section II.b. of this paper, (encouraging appropriate legal and professional education).

<sup>106</sup> Some proponents of the substantial use of cryptography retort by asking whether cryptography is more costly than a courier or a safe to protect an original?

<sup>107</sup> Although market-based arguments against implementing new or stronger security mechanisms prevail, there is evidence that market demand for security products appears to have accelerated considerably. This position is cautiously, yet optimistically, presented in light of the many "false starts" which security market pundits' reports have historically missed.

<sup>108</sup> For example, NIST plans to "[i]nvestigate the economic interests involved in the DSS." Miles Smid, "draft Response to comments on the NIST proposed digital signature standard," presented at Crypto '92 (Santa Barbara, Aug. 17, 1992) at 13. Note that the Data Encryption Standard (DES) "reflects hundreds of millions of dollars in investment," Geoffrey Turner, SRI, quoted in "Board to review U.S. policy on use of cryptography." *Network World*, Sept. 21, 1992 at 92.

SOURCE OF COST	APPLICABLE COST CONSIDERATIONS
<ul style="list-style-type: none"> <li>•Crypto. software licensing</li> <li>•Certificate purchasing</li> <li>•Export filing process</li> </ul>	<ul style="list-style-type: none"> <li>•License negotiation</li> <li>•Certificate purchase costs</li> <li>•Legal and technical fees for export license</li> <li>•Perhaps these are diminishing issues if Software Publisher's Association-type policies &amp; agreements proliferate, and export reform continues</li> </ul>
<ul style="list-style-type: none"> <li>•Additional cryptographic communications overhead</li> </ul>	<ul style="list-style-type: none"> <li>•Size of transactions (if transaction volume is great and the size of each such transaction is small proportionally, cost is a greater factor)</li> <li>•Communicating certificates/CRLs, etc.</li> <li>•Interoperable functional standards implementation</li> </ul>
<ul style="list-style-type: none"> <li>•Professional training, staffing and support<sup>109</sup></li> </ul>	<ul style="list-style-type: none"> <li>•Comparatively few practitioners of the art</li> <li>•Considerable learning curve</li> <li>•Technical development nontrivial &amp; highly variable</li> <li>•Problems in reaching agreement on implications of certificates</li> <li>•User training and servicing</li> </ul>
<ul style="list-style-type: none"> <li>•Additional processing<sup>110</sup> and storage</li> </ul>	<ul style="list-style-type: none"> <li>•CRL, certificate and message signing and verification</li> <li>•Host-based cycles (expensive compared to PCs)</li> <li>•Time sensitivity of subject data (a big factor)</li> </ul>
<ul style="list-style-type: none"> <li>•Key and certificate management and operation</li> <li>•Export "diversion in place" oversight<sup>111</sup></li> </ul>	<ul style="list-style-type: none"> <li>•Liabilities of certificate issuer</li> <li>•Bonding and liabilities of "organizational notaries"</li> <li>•Issuance and revocation procedures, security and audit</li> <li>•Drafting and executing agreements and policies</li> <li>•Configuration management</li> </ul>

**TABLE 4 - SURVEY OF COSTS IN IMPLEMENTING CRYPTOGRAPHY**

Another cost issue requiring resolution is whether governments will develop, or make agreements with providers to supply cryptographic software to small businesses or to the disadvantaged. If so, would such software distribution be viewed as illegally "in competition" with private enterprise. Recent events associated with "enhanced" or "value-added" information service provision by the Federal Maritime Commission and other agencies highlight this point.<sup>112</sup> Finally, differences between private and public policy objectives should be

<sup>109</sup> One example is the training requirements under the Computer Security Act at 1987 Fed. Reg. 26,940 (June 12, 1991).

<sup>110</sup> See Ronald L. Rivest, "On NIST's Proposed Digital Signature Standard," PROCEEDINGS OF THE SECOND CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE (Washington, DC, June 1, 1992) § 4.5.5 (providing an analysis of cryptographic processing costs and notes "an approximate doubling of computer power (per dollar) every two years, and an approximate increase of a factor of 4500 after twenty-five years . . . . In the year 2017, I expect computer power will be about 5000 times cheaper than it is now.").

<sup>111</sup> An example of this is the costs associated with any requirements imposed on a network, and the costs to monitor or prevent actively the export of controlled technical data from the U.S. under the Export Administration Regulations.

<sup>112</sup> See generally O.M.B. Management of Federal Information Resources Proposed Revision of OMB Circular A-130. 57 Fed. Reg. (No. 83) 18,296 (Apr. 29, 1992); Tariffs and Service Contracts, Federal Maritime Commission, 57 Fed. Reg. 36,268-36,311 (Aug. 12, 1992).



considered since conflicting agendas affect the choices available in designing model security baselines.<sup>113</sup>

4. Private vs. Public - Another consideration is whether, and how, baselines in the private and public sectors should vary. For example, a private sector "business risks" model may not be necessarily applicable to public sector obligations in which public servants play a non-profit and fiduciary role to the public at large. In such an environment, there may be a more compelling basis for strong security.
5. Present vs. Future - Where costs of computing continue to decrease rapidly, where availability of computers and security mechanisms continue to increase rapidly, and where there is growing confidence that "open systems" environments will become typical, should baseline requirements be skewed towards the present or the future (assuming that any requirements necessarily cannot be totally neutral as to their placement in time)?
6. Conflicting Security Requirements - Where baseline security requirements (such as statute, regulation or agreement) conflict with a particular transaction's special security requirement(s), the special requirements should preempt baseline requirements.
7. The Party(ies) Requiring Protection or Assurances - Whether the party requiring assurances or protection (*e.g.*, against revocation or repudiation) is either the originator, the recipient or a third-party beneficiary should be considered. For example, if the originator requires specific security assurances, security requirements can arguably be less stringent than where the recipient also requires assurances. This is because the originator is in the better position to control the type and extent of the security applied.<sup>114</sup> The recipient must either accept or reject that which the originator sends. TABLE 5 presents a simplified (perhaps over-simplified) comparison of various document types, the effects of which should be reflected by the Model Security Baseline.<sup>115</sup> TABLE 5 is necessarily subjective -- because the primary beneficiary of security will depend upon the particular circumstances.

---

<sup>113</sup> For example, government goals in information security are typically not geared toward profit-oriented risk taking, but rather toward the prevention of fraud or other loss.

<sup>114</sup> Originators may (depending on the implementation) optionally include cryptographically enhanced security (*e.g.*, digital signatures) for their own protection even where not legally required to do so. Whereas, in the absence of agreement or rule, the recipient is at the mercy of the originator.

<sup>115</sup> See *infra* Section II.c. The Baseline adopts the term *message* for consistency with international standards. The term *transaction* or other descriptive term can be substituted by the user.

TYPE OF TRANSACTION	ORIGINATOR	RECIPIENT	BOTH	3RD PARTY BENEFICIARY
Complaint	X			
Credit EFT		X		
Debit EFT	X			
Deed   Will		X		X
Hazardous Waste Manifest	X			X
"I.O.U."		X		X
Notice			X	
P.O.   Contract			X	
Power of Attorney			X	X

**TABLE 5 - PRIMARY BENEFICIARY OF SECURITY**

### c. A Model Security Baseline

The following Model Security Baseline ("Baseline") is presented as one approach that contributes to the development of rules affording greater certainty for the following risk assumptions. The Baseline assumes that the transactions are largely procurement or commercial in nature, and that the anticipated electronic commerce environment may include open systems. For simplicity, the Baseline creates three classes of messages:<sup>116</sup> *Level 1*, *Level 2*, and *Level 3*, each requiring incrementally stronger security, such as the use of cryptographic methods for authentication, integrity, and confidentiality purposes.<sup>117</sup> Three levels are within the boundaries of workable rule-making. Where more than three classes of security are desired or required, greater granularity in the levels, or additional levels with stronger or weaker characteristics can be developed responsively. The Baseline also contemplates greater specificity in subsequently derived rules using the Baseline as a tool.<sup>118</sup>

Both legal and computer security circles have expressed concern that security requirements should be separated from the specific security technologies implemented.<sup>119</sup> Although the following Baseline may be critiqued as providing inadequate separation, it provides comparatively general (and flexible) requirements.

---

<sup>116</sup> These three classes of transactions are substantially consistent with the three classes of information in electronic form presented in TABLE 1 - COMPARISON OF SIGNED WRITINGS AND ELECTRONIC INFORMATION, *supra* Section II.c.

<sup>117</sup> The Baseline is intended to help navigate through the pivotal decision (and perhaps the most difficult policy controversy) of whether or not to require the use of cryptographic-based security mechanisms. The Baseline is reprinted in Appendix 1 without footnotes and other distractions.

<sup>118</sup> The Baseline provides a practical interface between policies and detailed rules. For example, the Baseline provides a roadmap for enforcing a security policy, and yet, it purposefully refrains from detailing cryptographic key size, levels of passwords, algorithms, whether hardware is needed to implement cryptography and other legal and security techniques, parameters and requirements. See *supra* TABLE 3 - RELATIVE LEVELS OF ABSTRACTION.

<sup>119</sup> Early drafts of the ABA Resolution, *supra*, expressly considered cryptographic technologies. This consideration precipitated concern within the legal community that by mentioning cryptographic technologies (i) the failure to use them would create exposure, and (ii) the rules would become antiquated prematurely.



## A MODEL SECURITY BASELINE - LEVEL 1

Section 1 - *Level 1 Message Attributes*. An electronically created, communicated, or stored message of the parties shall be considered a "Level 1" message where 1.a, 1.b, 1.c and 1.d are applicable – singularly or in any combination:

- 1.a. the message(s) does not contain highly sensitive information,<sup>120</sup> proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value<sup>121</sup> of the message(s) [over any [thirty (30)]<sup>122</sup> day period] [as established by the parties] [is not expected to exceed] [does not exceed] [five thousand dollars (\$5,000)]<sup>123</sup> [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. no applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or<sup>124</sup>
- 1.d. the message is not highly time sensitive.<sup>125</sup>

Section 2 - *Security/Reliability*. The security implemented for Level 1 messages shall include, at a minimum:

<sup>120</sup> The use of the Computer Security Act of 1987 as a threshold for baseline criteria raises issues (and possibly problems) because most EDI information can reasonably be considered sensitive under the Act. The Baseline seeks to accommodate sensitive information under the act – providing incrementally stronger security in its Levels.

<sup>121</sup> Value is intended to mean actual or fair market value. Notwithstanding this definition, legal damages, the value of a loss to society (e.g., environmental pollution – potentially intangible or difficult to ascertain), as well as issues of consequential damages should also be considered. *See infra* and 98; *Evra Corp. v. Swiss Bank Corp.*, 673 F.2d 951 (7th Cir. 1982) (failure of bank to properly handle telex wire transfer not liable for consequential damages because it had not been placed on notice of special circumstances giving rise to them).

<sup>122</sup> The [bracketed] portions of text in the Baseline indicate their optional character. In fact, as a model, all provisions in the Baseline are ultimately optional.

<sup>123</sup> The \$5,000 is intended to be an aggregate amount. Its purpose is to prevent "splitting" large orders into multiple smaller ones. The use of a value limit on multiple transactions has proven difficult to enforce because the anticipated value/volume for a future time period is speculative. Inflation will render the \$5,000 less important over time. A link to a government price index, such as the consumer price index might be useful. The author acknowledges that some knowledgeable legal and technical experts believe that an aggregate amount is either unnecessary or inappropriate.

<sup>124</sup> Additional criteria could provide that: "the business situation does not present unusual elements which tend to increase the risk above normal levels." However, determining the parameters of "normal levels" could be difficult or fruitless.

<sup>125</sup> *See supra* Section II.e. TRUSTED ENTITIES AND TIME STAMPING, regarding applications requires greater proof of timeliness. E.g., in *Interactive EDI*, "[f]aster EDI is a primary requirement. This is not only a requirement on the underlying communications methods, but on all functional entities within and between the trading partners . . . response times of seconds or fractions of a second, as opposed to minutes or hours, will generally be required." RECOMMENDATION TO UN/ECE/WP.4 ON INTERACTIVE EDI WITHIN THE CONTEXT OF UN/EDIFACT, TRADE/WP.4/R.842 (July 21, 1992) at 8.

- 2.a. noncryptographic identification and authentication [e.g., password-user ID];<sup>126</sup>
- 2.b. recognized controls to ensure authenticity,<sup>127</sup> integrity, [confidentiality,] and availability;<sup>128</sup> and
- 2.c. audit trails.<sup>129</sup>

Section 3 - *Legal Effect*. For all legal purposes, all Level 1 messages which are communicated pursuant to Section 2 shall be presumed [conclusively?<sup>130</sup>] to be "in writing," "signed,"<sup>131</sup> authentic, and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.<sup>132</sup>

Level 2 and 3 messages require stronger security. The following Baseline affords Level 2 messages greater security. Enhancement of Level 1 requirements is achieved through the addition of the use of cryptographic methods for MACs or digital signatures, and optionally for stronger confidentiality protection. Additions and deletions to Baseline Level 1 messages are noted accordingly.

<sup>126</sup> "Noncryptographic identification and authentication" requires greater specificity such as by reference to National Institute of Standards and Technology (NIST) or other authoritative guidelines. Depending upon the implementation, security should minimally be of the "C2" level where the passwords are associated with an individual. Class C2: Controlled Access Protection makes "users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation." DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, DOD 5200.28-STD (Dec., 1985)(hereinafter "DoD Trusted Criteria") at 15.

<sup>127</sup> Levels 1 and 2 of the Baseline do not accommodate full non-repudiation because of their lack of a trusted time stamp. *See supra* Section II.d. and II.e.. (concerning non-repudiation and trusted time stamps).

<sup>128</sup> Such controls should be comparable to recognized and appropriate criteria, e.g., in the nature of certain requirements included within the Class C2 Security Policy. *See* DoD Trusted Criteria *supra* at 15.

<sup>129</sup> Each entity participating in a transaction (e.g., each trading partner and all intermediaries) should be required to keep an audit trail. *See generally* A GUIDE TO UNDERSTANDING AUDIT IN TRUSTED SYSTEMS, National Computer Security Center, NCSC-TG-001 Version 1 (July 28, 1987); BELDEN MENKUS and ZELLA G. RUTHBERG, CONTROL OBJECTIVES, (EDP Audit Foundation, 1990).

<sup>130</sup> Issues associated with conclusive presumptions are discussed in Section IV. *infra* BURDEN OF PROOF AND PRESUMPTIONS.

<sup>131</sup> Where the message's originator intended the message to be signed and properly communicated, otherwise the presumption shall be that the transaction was intended to be in writing but not signed. A careful review of the purpose of each particular signature requirement must be undertaken; and the parties should be confident that the particular purpose of the signature requirement is met by the substituted electronic mechanisms.

<sup>132</sup> *See* BAUM AND PERRITT, *supra* at 185-186.



## A MODEL SECURITY BASELINE - LEVEL 2

Section 1 - *Level 2 Message Attributes*. An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 2" message where 1.a, 1.b, 1.c and 1.d are applicable – singularly or in any combination:

- 1.a. the message ^ contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is ^ expected to exceed] [^ exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. ^ applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or
- 1.d. the message is not highly time sensitive.

Section 2 - *Security/Reliability*. The security implemented for Level 2 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [e.g., password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c. audit trails; and
- 2.d. [message authentication codes (MACs)]<sup>133</sup>, [digital signatures] [and/or encryption for confidentiality].<sup>134</sup>

Section 3 - *Legal Effect*. For all legal purposes, all Level 2 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

The following Level 3 messages have attributes which require "trusted third party" security services. Additions and deletions to Level 2 are noted. The satisfaction of other legal requirements, such as negotiability, will require alternative security services.<sup>135</sup>

<sup>133</sup> This may involve using secret key techniques such as DES (see FIPS-PUB 46-1). See FIPS-PUB 113 on MACs.

<sup>134</sup> This may be accomplished through the use of public key-based or conventional key-based key management and key exchange mechanism to transmit/create secret session keys for privacy of messages.

<sup>135</sup> A trusted record keeper is anticipated to be necessary to accommodate computer-based negotiable documents. See BAUM AND PERRITT *supra* at § 5.11 "-Documentary Transfers," and § 11.9 "-Negotiability and Bills of Lading" (addressing trusted record keeping mechanisms for negotiable documents); TABLE 1 - COMPARISON OF SIGNED WRITINGS AND ELECTRONIC INFORMATION, *supra* at Section II.c.

## A MODEL SECURITY BASELINE - LEVEL 3

Section 1 - *Level 3 Message Attributes*. An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 3" message where 1.a, 1.b, 1.c, 1.d and 1.e are applicable – singularly or in any combination:

- 1.a. the message ^ contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is ^ expected to exceed] [^ exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. ^ applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message;
- 1.d. the message is ^ highly time sensitive; or
- 1.e. an acknowledgment by a notary public, or comparable "stronger" proofs or certifications is required.

Section 2 - *Security/Reliability*. The security implemented for Level 3 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [e.g., password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c. audit trails;
- 2.d. [message authentication codes (MACs)], [digital signatures] [and/or encryption for confidentiality]; and
- 2.e. electronic notarization (time stamping and [MAC<sup>136</sup>] [digital signature]) by a trusted entity.

Section 3 - *Legal Effect*. For all legal purposes, all Level 3 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

As presented, Section 3 - *Legal Effect* (of all three Baseline levels) focuses on assuring that computer-based messages are afforded comparable legal effect to paper-based messages. However, because Baseline Levels 2 and 3 use incrementally stronger security mechanisms (than in Level 1) that provide greater assurances of

<sup>136</sup> There is not yet a viable infrastructure to support symmetric-based key management where several hundred thousand parties utilize a security mechanism. Also, notarization using MACing with symmetric key technology requires that verification of notarization must be provided exclusively by the notary since keys in such an implementation cannot be shared.



trustworthiness, there is a compelling basis for providing other beneficial legal effects within Section 3 - *Legal Effect*. Consequently, as an alternative, Baseline legal effects should provide incrementally stronger legal presumptions and burden allocations. For example, where a party used a digital signature, the authenticity and integrity of the computer-based information should be more difficult to attack legally (or rebut) than if weaker security had been applied to the message. The following two sections consider these issues in more detail and present such a proposal.

#### IV. BURDEN OF PROOF AND PRESUMPTIONS

*There is no satisfactory test for allocating the burden  
of proof in . . . any given issue.*<sup>137</sup>

Scant attention has been paid to burden of proof and presumption issues in electronic commerce. This is unfortunate since, after all, proof issues are at the heart of the meaningful resolution of disputes. Burden of proof and presumption issues have been approached largely without meaningful consideration of the *dynamic* proof sets<sup>138</sup> necessary to accommodate transaction-oriented environments. Dynamic proof sets differ sharply from the relatively *static* proof sets developed for record-oriented environments. While undeniably a daunting task, and an issue worthy of further study, burdens of proof and presumptions must be examined and integrated into a workable legal framework for electronic commerce.<sup>139</sup>

The development of electronic commerce rules are intimately affected by burden of proof requirements which consist of both the *risk of nonpersuasion* and the *duty of producing evidence*.<sup>140</sup> Burden of proof issues affect (i) electronic message reliability and genuineness, and (ii) admissibility and enforceability<sup>141</sup> of information in electronic form (e.g., substituted for paper-based documentation).

In developing and evaluating rules governing electronic commerce, one must recognize that "[t]he burden of pleading [should be] allocated on the basis of pragmatic considerations of fairness, convenience, and policy, rather than on any general principle of pleading."<sup>142</sup> Yet, in many respects, the law's approach to the rules governing proof of facts at trial, as exemplified by the U.C.C., has been critiqued as:

---

<sup>137</sup> GEOFFREY C. HAZARD, JR., CIVIL PROCEDURE, 322 (3rd ed. 1985) [hereinafter, "HAZARD"].

<sup>138</sup> Telephone interview with Gregory P. Joseph, Esq., (Oct. 10, 1992).

<sup>139</sup> For example, maritime law is rich in presumptions because there are often no witnesses to events on the high seas. Furthermore, cargo is, as a matter of course, passed through many hands internationally.

<sup>140</sup> See HAZARD *supra* at 314. U.C.C. § 1-201(8) states that the *Burden of establishing* "a fact means the burden of persuading the triers of fact that the existence of the fact is more probable than its non-existence."

<sup>141</sup> Electronic commerce legal commentators have often focused either on "enforceability" or on "evidentiary value."

<sup>142</sup> HAZARD, *supra* at 323.

remarkably casual, indeed almost haphazard. There are no general provisions constructing the evidentiary relationships of the parties, and the UCC's specific rules are insufficient to provide guidance on a host of significant and recurring problems. Predictably, the result has been that the goals of consistency and clarity in commercial law have not been achieved in the important area of evidentiary proof rules.<sup>143</sup>

One rule allocates the burden of proof to the party having the readier access to knowledge about the fact in question.<sup>144</sup> In electronic commerce, this party may vary considerably depending on the computer involved, communications architecture, applications, and the party intended to benefit from the electronic message, among other considerations.

The Federal Rules of Evidence delineate presumptions.<sup>145</sup> Presumptions are "occasionally used to refer to the logical inference of one fact from the existence of another."<sup>146</sup> For example, "[i]f Smith mails at a postbox a letter to Jones, with proper address and postage on the envelope, the trier may infer that Jones received the letter."<sup>147</sup> Similarly, "[i]t has been declared that there is a presumption, not conclusive, of prompt delivery of a letter mailed in the absence of evidence to the contrary."<sup>148</sup> "The degree of persuasion required is also sometimes manipulated as a handicap against disfavored contentions. Thus if a claim is presented that a written contract was orally modified, the party claiming the modification must in some jurisdictions prove its contention by clear and convincing evidence."<sup>149</sup>

"What, then, are the bases upon which courts or legislatures will create presumptions? For the most part they are the same kinds of reasons that influence the allocation of the production burden generally, and these may be summed up as reasons of convenience, fairness, and policy."<sup>150</sup> Additionally, distinctions in

---

143 Ronald J. Allen and Robert A. Hillman, *Evidentiary Problems in - and Solutions for - The Uniform Commercial Code*, 1984 Duke L. J. 92, 93.

144 HAZARD, *supra* at 324.

145 "In all civil actions and proceedings not otherwise provided for by Act of Congress or by these rules, a presumption imposes on the party against whom it is directed the burden of going forward with evidence to rebut or meet the presumption, but does not shift to such party the burden of proof in the sense of the risk of nonpersuasion, which remains throughout the trial upon the party on whom it was originally cast." FED. R. EVID. 301 "PRESUMPTIONS IN GENERAL IN CIVIL ACTIONS AND PROCEEDINGS."

146 9 WIGMORE *supra* at § 2492; See *F.A.R. Liquidation Corp. v. Brownell*, 140 F.Supp. 535 (D.DE 1956) (permitting inference based on fact established by direct or circumstantial evidence of time telegram communicated).

147 HAZARD, *supra* at 326.

148 *Franklin Life Ins. Co. v. Brantley*, 165 So. 834 (AL 1936); see *Kiker v. Commissioner of Internal Revenue*, 218 F.2d 389, 393 (4th Cir. 1955) (there was no presumption that a letter was delivered in the ordinary course of the mails where address was not proper).

149 HAZARD, *supra* at 325.

150 HAZARD, *id.* at 328.



constitutional and procedural requirements for burdens of proof and presumptions in civil versus criminal proceedings must be considered.<sup>151</sup>

The use of presumptions affecting validity or enforceability of information in electronic form are widespread in EDI agreements. One example is the Model Electronic Payments Agreement and Commentary ("Model Agreement"), which states that "[t]he receipt by the sender of an acknowledgment from the recipient shall constitute *conclusive evidence* that the subject communication was received and is syntactically correct."<sup>152</sup> The practical effect of a conclusive presumption<sup>153</sup> is to excuse the sender from proving receipt where the proof is entirely in the recipient's control, perhaps to do otherwise would render EDI commercially ineffective.<sup>154</sup>

To what extent should *conclusive presumptions* be subject to attack?<sup>155</sup> How much evidence should be required to disprove or shift a presumption? By analogy, take the case of the mails. "If, for example, the addressee of a properly mailed letter testifies that he or she never received it, that testimony would, if believed, justify a finding of nonreceipt." "[T]he destruction of the presumption would not, however, compel a finding of non-receipt because a properly addressed letter is so likely to reach its destination that a rational inference may be drawn that it did so."<sup>156</sup> Should such a presumption hold in electronic commerce matters? And, to what extent should or must there be a *rational connection* between the fact presumed and the fact proved? To illustrate the approaches taken in many domestic and international model electronic commerce agreements, the Commentary to the Model Electronic Payments Agreement presents the following addition presumptions:

Validity and Enforceability. Neither party shall contest the validity or enforceability of Transaction Sets or notices communicated pursuant to this Agreement on grounds related to the absence of paper-based writings, signings or originals.

---

<sup>151</sup> E.g., Hazard notes "an intermediate test which is occasionally applied in civil controversies" — "clear and convincing evidence." See Notes of Advisory Committee of the 1972 Proposed Rules, FED. R. CIV. P. 301.

<sup>152</sup> MODEL AGREEMENT, *supra* at Section 6.3, and MODEL EDI TRADING PARTNER AGREEMENT *supra* at § 2.2., Comment 7.

<sup>153</sup> "The *conclusive presumption* is not really a procedural device at all. Rather it is a process of concealing by fiction a change in the substantive law. When the law conclusively presumes the presence of B from A, this means that the substantive law no longer requires the existence of B in cases where A is present, although it hesitates as yet to say so forthrightly. (emphasis added). 9 WIGMORE *supra* at § 2492; and Gordon and Tenenbaum, "Conclusive Presumption Analysis: The Principal of Individual Opportunity," 71 NW. U. L. REV. 579 (1976).

<sup>154</sup> However, the parole evidence rule does permit the voluntary adoption of a "super parole evidence rule" that prevents the parties from using evidence of future oral modifications. See U.C.C. § 2-202 "Final Written Expression: Parol or Extrinsic Evidence."

<sup>155</sup> By definition, *conclusive presumptions* are irrefutable, yet in practice, they are sometimes refutable.

<sup>156</sup> HAZARD. at 330; 9 WIGMORE, *supra* at § 2489. Given the various documented instances where mail is destroyed or delayed, this presumption is suspect.

Each Transaction Set and notice communicated in electronic form pursuant to this Agreement shall be considered to be:

- (a) "in writing" and "written" to an extent no less than if in paper form;
- (b) "signed" where the signer includes data intended as a signature [as agreed among the parties] to an extent no less than if conventionally undertaken with pen and paper; and
- (c) an original.<sup>157</sup>

Examples of other instructive presumptions include the following:

- i. If EDI messages are transmitted in accordance with an authentication procedure such as a digital signature, they shall have, between parties, a comparable evidentiary value to that accorded to a signed written document.<sup>158</sup>
- ii. In an action with respect to an instrument, the authenticity of, and authority to make, each signature on the instrument is admitted unless specifically denied in the pleading. If the validity of a signature is denied in the pleadings, the burden of establishing validity is on the person claiming validity, but the signature is presumed to be authentic and authorized unless the action is to enforce the liability of the purported signer and the signer is dead or incompetent at the time of the trial of the issue of validity of the signature.<sup>159</sup>
- iii. If there is a discrepancy between the terms of the payment order transmitted to the system and the terms of the payment order transmitted by the system to the bank, the terms of the payment order of the sender are those transmitted by the system.<sup>160</sup>
- iv. A document in due form purporting to be a bill of lading . . . or any other document authorized or required by the contract to be issued by a third party shall be prima facie evidence of its own authenticity and genuineness and of the facts stated in the document by the third party.<sup>161</sup>

---

<sup>157</sup> MODEL AGREEMENT, *supra* at § 6, Comment 13.

<sup>158</sup> TEDIS, EUROPEAN MODEL EDI AGREEMENT, ART. 10 (Final Draft, 1991).

<sup>159</sup> U.C.C. § 3-308(a) ("Proof of Signatures and Status as Holder in Due Course.") "The presumption rests upon the fact that in ordinary experience forged or unauthorized signatures are very uncommon, and normally any evidence is within the control of, or more accessible to, the defendant." *Id.* Official Comment 1.

<sup>160</sup> U.C.C. § 4A-206 ("Transmission of Payment Order through Funds-Transfer or Other Communications System.").

<sup>161</sup> U.C.C. § 1-202 ("Prima Facie Evidence by Third Party Documents.").



The Model Security Baseline<sup>162</sup> includes presumptions which may vary, and which deserve further scrutiny. One immediate issue is whether the Baseline (as well as the various EDI-related model agreements) should delve further into burdens of proof and other evidentiary matters. If incrementally greater security mechanisms are used (such as in Model Baseline Levels 2 and 3), *why should not the parties receive incrementally increased presumptions as to the admissibility, credibility and weight to be afforded such messages?*<sup>163</sup> For example, TABLE 6 proposes replacing (alternatively, adding to) the Model Baseline's Section 3 - *Legal Effect* with the following presumptions for certain classes of messages. This is intended to provide a more dynamic risk-based model, and provide stronger security users with appropriate and commensurate benefits.<sup>164</sup>

MODEL BASELINE SECTION 3, LEVEL:	PRESUMPTION	(SUBSTITUTE SECTION 3 - LEGAL EFFECT)
1	Rebuttable Presumption A	Shifts burden of proof to rebut presumption by a <i>preponderance of the evidence</i>
2	Rebuttable Presumption B	Requires <i>clear and convincing</i> proof to rebut presumption of authenticity
2A (alternative to 2)	Rebuttable Presumption C	Requires proof <i>beyond a reasonable doubt</i> to rebut presumption of authenticity
3	Irrebuttable Presumption	Presumption is conclusive regardless of the opponent's evidence

TABLE 6 - SUBSTITUTE MODEL BASELINE SECTION 3 - LEGAL EFFECT<sup>165</sup>

TABLE 6 may be preferable to the Baseline's *Section 3 - Legal Effect*, because the TABLE 6 presumptions are not inherently tied to conventional paper-based technologies. Finally, the increasing strengths of the presumptions in Table 6 are more dynamic than those of the Baseline and can be used in a multidimensional scheme.<sup>166</sup> Consequently, TABLE 6 deserves further consideration.

<sup>162</sup> Section III.c., *supra*.

<sup>163</sup> There is strong basis in the law for providing greater legal effect to documents which have been more strongly authenticated or secured; this is the case with self-proving wills and some statutes of limitations.

<sup>164</sup> It has been comically suggested that "as you move much beyond three to four levels of burdens of proof, no one except Judge Wapner could possibly understand and effectively use it." Interview with Alfred I. Maleson, Prof. Emeritus, Suffolk Univ. Law School, in Boston (Nov. 4, 1992).

<sup>165</sup> Transactions which do not satisfy the security criteria of Baseline Level 1 could, depending upon the legal scheme, be viewed as representing *simple presumptions* which shift the burden of going forward with the evidence, but do not change the burden of proof.

<sup>166</sup> For example, a scheme could be developed where a Baseline Level 1 transaction uses Level 2 security and therefore responds to a stronger presumption.

## V. INTEGRATING FORMALISTIC & EVIDENTIARY REQUIREMENTS

Legal requirements for information in electronic form are typically evaluated from one of two perspectives: (i) formalistic-related requirements (e.g., focusing on requirements for, or the sufficiency of, substitutes for "signed writings"),<sup>167</sup> or (ii) evidentiary-related requirements (focusing on admissibility, credibility and proof issues).<sup>168</sup> Where these perspectives are either viewed in a vacuum or adopted without contemplating their interrelationship, the resulting perspective and rules are destined to be dysfunctional. Insufficient attention has been directed toward utilizing an integrated *cradle-to-grave* analysis of the total electronic commerce environment and its requirements. To aid such an analysis, FIGURE 1 presents a representative cradle-to-grave analysis of a transaction. FIGURE 1 segments electronic commerce transactions into four phases of legal import: Phase 1-Creation (includes processing), Phase 2-Communication, Phase 3-Verification (includes retention functions)<sup>169</sup> and Phase 4-Dispute Resolution <sup>170</sup>

---

<sup>167</sup> See Section II.a. "Treatment in the Law" *supra*.

<sup>168</sup> See Section IV. "BURDEN OF PROOF AND PRESUMPTIONS," *supra*.

<sup>169</sup> Transaction record storage would logically follow Phase 1 - verification -- and verification might be undertaken following each use of the stored information.

<sup>170</sup> In this hypothetical transaction: [Phase 1] a user creates information in electronic form to which some signature or authentication mechanism is used to satisfy legal requirements and to mitigate security threats. Then, optionally, the document is witnessed or cosigned or both, and if necessary, notarized (perhaps via a trusted crypto. box). [Phase 2] Next, the document is communicated to the intended recipient via third party service provider. The recipient then accesses and obtains the message. [Phase 3] The recipient then verifies the message for assurances of authenticity using one or more of a variety of verification techniques. Following verification, the recipient optionally can communicate an acknowledgment back to the originator such as a functional acknowledgment to notify the originator that the message was received and syntactically correct. Also, where the transaction is contractual in nature, the recipient can communicate an acceptance. [Phase 4] Should a dispute ensue, the parties present admissible evidence to the dispute resolution mechanism and seek to persuade the fact finder, in part, by the weight and credibility of the evidence. A decision by the fact finder completes the hypothetical.



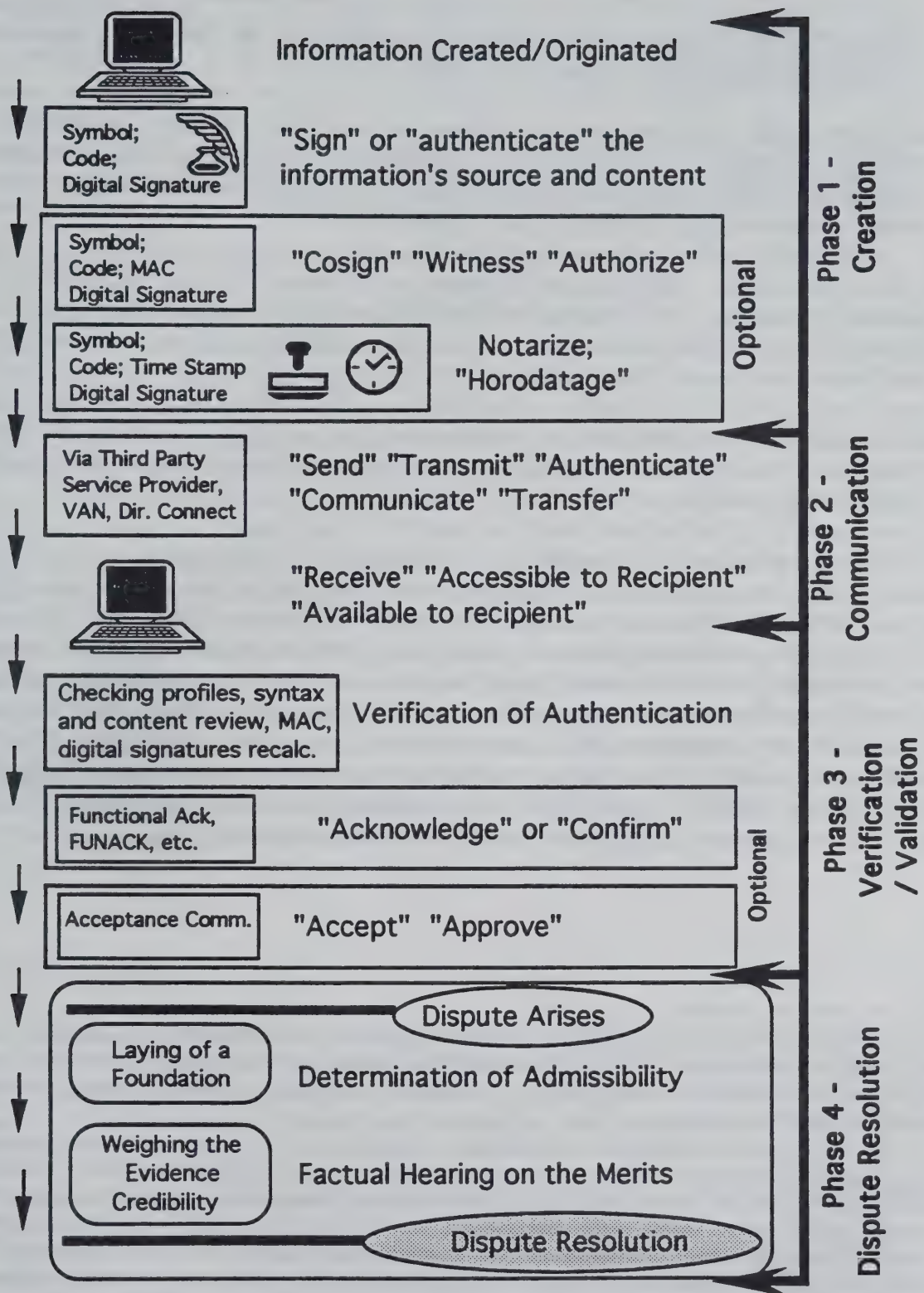


FIGURE 1 - A HYPOTHETICAL CRADLE-TO-GRAVE TRANSACTION

The remainder of this Section begins considering the following questions -- questions that deserve study beyond this paper:

a. If formalistic requirements are reduced or eliminated<sup>171</sup> (e.g., at Phase 1, FIGURE 1), will the evidentiary requirements of laying a foundation (preliminary evaluation of authenticity and relevancy) necessarily shift to a factual determination of weight and credibility?<sup>172</sup>

b. If so, will such a shift either increase or decrease the total quantum of proof required (e.g., at Phase 4, FIGURE 1) from either party. Further, will it qualitatively shift the *status quo* to the unintended or unjustified disadvantage of one of the parties?

c. Should the evidentiary requirements for laying a foundation be minimized, thereby further rendering the litigation to one of credibility and weight of the evidence?

If both formalistic and evidentiary foundational requirements are minimized, it is likely that a new risk will be created because the total required quantum of proof (weight and credibility) may increase. The party seeking to introduce a document cannot pre-gauge the extent of the required proof. The party cannot therefore rely on otherwise existing relatively static proof requirements. Absent definable and widely recognized formalistic requirements for electronic commerce, the current formalistic requirements for paper-based documents become less predictable. Theoretically, the potential evidentiary requirements, including the burden of proving transactions, become infinite. TABLE 7, presents some of the proffered relationships between formalistic, evidentiary foundational, and proof requirements.<sup>173</sup>

---

<sup>171</sup> For example, these include requirements for a signatures, or their electronic analogs for the creation of enforceable documents in electronic form. If requirements for a signature are replaced by requirements for an electronic analog, then, the formalistic requirements remain, however, they simply take on a new form -- an electronic form.

<sup>172</sup> The elimination of formalistic requirements is not out of step with modern legal developments. "What is valued is not form for form's sake, but useful form." LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 278 (Touchstone Book, 2nd ed. 1965) "The statute of frauds survived; other formalities, which had no useful place, disappeared from the law of contract." "In general, sentiment and tradition had little place in commercial law; what survived was the fit and the functional." *Id.* at 279. It is precisely the signature, of course, which is alleged by many contemporary scholars and practitioners to be formalistic, unfit and dysfunctional.

Similarly, "[t]he advantage of the writing was not only that it furnished better proof. . . but also that it made it possible to enforce obligations for which there would otherwise have been no proof at all." OLIVER WENDELL HOLMES, THE COMMON LAW 262 (1881).

<sup>173</sup> Perhaps the most tenuous of relationships is between foundational and proof requirements. An accurate description of the relationship is difficult to draft. However, the relative effects between formalistic requirements and evidentiary requirements are better substantiated.



STATUTE OF FRAUDS OR COMPARABLE FORMALISTIC REQUIREMENTS		RELATIVE STRICTNESS OF REQUIREMENTS OF LAYING A FOUNDATION FOR ADMISSIBILITY		ANTICIPATED EFFECT ON THE QUANTUM OF PROOF (WEIGHT & CREDIBILITY) TO ENSURE ENFORCEABILITY
Yes	+	Greater	=	Lesser
No	+	Greater	=	Medium
No	+	Lesser <sup>174</sup>	=	Greater

TABLE 7 - EFFECT OF DIFFERING FORMALISTIC & FOUNDATIONAL REQUIREMENTS

Some commentators propose that all information in electronic form should be admitted into evidence.<sup>175</sup> Under this view, the judicial process almost exclusively involves the fact finder determining the credibility of the evidence *without* the prerequisite of meaningfully laying a foundation. Alternatively, if a foundation were required, then it would be, a largely perfunctory requirement to minimize clearly irrelevant and prejudicial materials under Fed. R. Evid. 104(a) "Questions of Admissibility Generally" and Fed. R. Evid. 403 "Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time", respectively. Consequently, the inquiry into reliability and trustworthiness would no longer be bifurcated into (i) laying a foundation as a prerequisite to admissibility, and (ii) determining the weight and credibility of the evidence.<sup>176</sup> Table 7 illustrates the anticipated dynamics of the trade-offs between these differing policies. One interpretation suggests that the diminution of formalistic and foundational requirements (the elimination of Statute of Frauds-like requirements and the relaxation of evidentiary foundation requirements) may not necessarily reduce electronic commerce barriers and costs. One euphemism which characterizes this concept is that there is *no free lunch*. What one tends to gain in the "Creation Phase" of the transactions (*see* FIGURE 1), is later lost by a commensurate increase in "Proof Phase" requirements.

## VI. CONCLUSION

This paper recognizes the contribution of appropriate security techniques, procedures and practices to the legal efficacy of electronic messages and records. There is an inherent linkage between security and legal efficacy that is not adequately appreciated. The security of electronic messages and records is not only a business

<sup>174</sup> The author recognizes that judiciary is likely to always demand some evidentiary foundation oversight.

<sup>175</sup> One commentator advocates that "for business records virtually everything should be admissible, unless it is inherently unreliable - and even then I have doubts about the wisdom of creating a rule applying to EDI that would exclude any evidence . . . . Exclusion due to inadmissibility is a drastic sanction that can deprive a party of its fundamental proofs." Letter from George F. Chandler, III, Esq. to Michael S. Baum (Sept. 10, 1992) (on file with author).

<sup>176</sup> In practice, however, the bifurcation has sometimes been blurred. "Any evidentiary shortcoming [in developing a foundation for admission of printouts from a computer retrieval system in drug prosecution] became a matter of weight to be given to the evidence rather than one of admissibility." U.S. v. Scholle, 553 F.2d 1109, 1124-25 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977).

requirement,<sup>177</sup> but also is an underlying legal requirement. Defining this linkage is indispensable to the rational and pragmatic development of reliable electronic commerce. When the law determines what is sufficiently secure, it must consider the particular message's risks and purpose(s). Legal requirements should clarify *reasonable security procedures* without sacrificing needed flexibility. It is not a question of "having security" or "not having security" rather, it is a question of the *strength* of the security mechanisms implemented. When this legal-security linkage becomes broadly recognized, then the progress in the law which the electronic commerce community deserves and demands will begin.

\*\*\*

---

<sup>177</sup> "Clearly, security is an essential business requirement and is, therefore, at the heart of UN/EDIFACT." UN/EDIFACT Security JWG, Draft Rec. for Security (Jul. 1992).



## APPENDIX - THE MODEL SECURITY BASELINE GRAPHICS

### A SECURITY BASELINE - LEVEL 1

**Section 1 - *Level 1 Message Attributes.*** An electronically created, communicated, or stored message of the parties shall be considered a "Level 1" message where 1.a, 1.b, 1.c and 1.d are applicable -- singularly or in any combination:

- 1.a. the message(s) does not contain highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is not expected to exceed] [does not exceed] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. no applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message;  
or
- 1.d. the message is not highly time sensitive.

**Section 2 - *Security/Reliability.*** The security implemented for Level 1 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [e.g., password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability; and
- 2.c. audit trails.

**Section 3 - *Legal Effect.*** For all legal purposes, all Level 1 messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic, and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.

## A SECURITY BASELINE - LEVEL 2

**Section 1 - Level 2 Message Attributes.** An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 2" message where 1.a, 1.b, 1.c and 1.d are applicable -- singularly or in any combination:

- 1.a. the message contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period] [as established by the parties] [is expected to exceed] [exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message; or
- 1.d. the message is not highly time sensitive.

**Section 2 - Security/Reliability.** The security implemented for Level 2 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [e.g., password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c. audit trails; and
- 2.d. [message authentication codes (MACs), [digital signatures] [and/or encryption for confidentiality].

**Section 3 - Legal Effect.** For all legal purposes, all Level 2 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.



## A SECURITY BASELINE - LEVEL 3

**Section 1 - Level 3 Message Attributes.** An electronically created, communicated, or stored message(s) of the parties shall be considered a "Level 3" message where 1.a, 1.b, 1.c, 1.d and 1.e are applicable – singularly or in any combination:

- 1.a. the message contains highly sensitive information, proprietary trade secrets, or other information requiring strong privacy protection;
- 1.b. the value of the message(s) [over any [thirty (30)] day period[ [as established by the parties] [is expected to exceed] [exceeds] [five thousand dollars (\$5,000)] [twenty-five thousand dollars (\$25,000)] [X dollars];
- 1.c. applicable law specifies alternative security measures, or otherwise preempts the applicability of the Model Baseline for the specified message;
- 1.d. the message is highly time sensitive, or
- 1.e. an acknowledgment by a notary public, or comparable "stronger" proofs or certifications is required.

**Section 2 - Security/Reliability.** The security implemented for Level 3 messages shall include, at a minimum:

- 2.a. noncryptographic identification and authentication [e.g., password-user ID];
- 2.b. recognized controls to ensure authenticity, integrity, [confidentiality,] and availability;
- 2.c. audit trails;
- 2.d. [message authentication codes (MACs)], [digital signatures] [and/or encryption for confidentiality]; and
- 2.e. electronic notarization (time stamping and [MAC] [digital signature]) by a trusted entity.

**Section 3 - Legal Effect.** For all legal purposes, all Level 3 Baseline messages which are communicated pursuant to Section 2 shall be presumed [conclusively?] to be "in writing," "signed," authentic and enforceable to no less an extent than if such messages had been undertaken using conventional (paper-based) mechanisms.





## APPENDIX B - "THE EDI CLEARINGHOUSE"

*The EDI Clearinghouse begins on the next page.*

Excerpted from: Electronic Contracting, Publishing, and EDI Law, Michael S. Baum and Henry H. Perritt, Jr., ©1991, Wiley Law Publications. Reprinted by permission of John Wiley & Sons, Inc.





# ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW

---

MICHAEL S. BAUM

Member of the Bar  
of the State  
of Massachusetts

HENRY H. PERRITT, JR.

Professor of Law  
Villanova University  
School of Law



Wiley Law Publications  
JOHN WILEY & SONS, INC.

New York • Chichester • Brisbane • Toronto • Singapore





# THE EDI CLEARINGHOUSE

Michael S. Baum

§ 5.1	Introduction
§ 5.2	Conventional Clearinghouses and Third-Party Service Providers
§ 5.3	Clearinghouse-like Implementations
§ 5.4	—Health Care
§ 5.5	—Payment Intermediaries
§ 5.6	—Bank Card Clearing Services
§ 5.7	—Commercial Aviation
§ 5.8	—Defense Department's Electronic Commerce and Treasury Department's Vendor Express
§ 5.9	—Securities Trading
§ 5.10	—Floral Delivery
§ 5.11	—Documentary Transfers
§ 5.12	—UCC Security Interest Filings
§ 5.13	Clearinghouse Services
§ 5.14	Clearinghouse Enforceability Services
§ 5.15	—Record Holding and Audit Trail
§ 5.16	Clearinghouse Structure
§ 5.17	Clearinghouse Connections
§ 5.18	—Direct Intermediary Clearinghouse
§ 5.19	—Indirect, Record-Holder Clearinghouse
§ 5.20	—TPSP Transfer Clearinghouse
§ 5.21	—Second-Level TPSP Clearinghouse
§ 5.22	Part and the Clearinghouse
§ 5.23	Clearinghouse Functions Without Cryptography
§ 5.24	—Key Management and the Clearinghouse
§ 5.25	—Public Key Certificate Management
§ 5.26	Clearinghouse Expediting Services
§ 5.27	—Database and Information Services
§ 5.28	Directory Services and the Clearinghouse

- § 5.29 —Business Information Attribute
- § 5.30 —Naming
- § 5.31 Conformance and Other Testing
- § 5.32 —Interoperability Testing
- § 5.33 —Testing Certifications
- § 5.34 —Testing Responsibilities
- § 5.35 —Transaction Flow Testing
- § 5.36 —The Clearinghouse and Testing
- § 5.37 Contract Determinative Services
- § 5.38 —Standard Generalized Markup Language
- § 5.39 Clearinghouse Regulatory Considerations
- § 5.40 —Antitrust Considerations
- § 5.41 —Essential Facilities Doctrine
- § 5.42 —Clearinghouse as Joint Venture
- § 5.43 —Telecommunications Regulatory Issues
- § 5.44 Standards Participation by the Clearinghouse
- § 5.45 —Clearinghouse Guideline Making
- § 5.46 —Overcoming Regulatory Road Blocks
- § 5.47 Clearinghouse Confidentiality Issues
- § 5.48 —Clearinghouse Agency Status
- § 5.49 Clearinghouse Forecast

## § 5.1 Introduction

An electronic data interchange (EDI) clearinghouse is envisioned as an administrative, legal, and technical infrastructure that provides various telecommunications and computer-based commercial trading services to bolster the reliability and enforceability of electronic transaction records, reduce legal uncertainty, and generally facilitate electronic trade. The EDI clearinghouse could provide a generalized framework to facilitate trade between established trading partners, as well as trading parties without benefit of prior dealings or privity of contract (open traders). To this end, the clearinghouse could provide an array of pretransaction, transaction, and transaction assurance services. (Pretransaction services allow prospective trading partners to determine whether and how to do business with each other. Transaction services bolster contract formation and administration. Transaction assurance services further reduce liability exposure.)

EDI clearinghouse services will extend well beyond traditional clearinghouse functions to enjoy broad-based support as a trusted entity. An EDI clearinghouse could potentially provide multiple services across broad markets on an interindustry basis. Nonetheless, the scope of clearinghouse

services implemented will depend upon available technology, legal<sup>1</sup> and security requirements, potential liability, the availability of insurance, and, of course, business needs and costs. Questions about which clearinghouse structures are best suited to EDI applications remain unresolved. For example, disagreement exists as to whether clearinghouses should provide interindustry or industry-specific services and whether there should be many or few clearinghouses.<sup>2</sup>

Notwithstanding these questions, the EDI clearinghouse promises significant benefits. This chapter presents an overview of possible EDI clearinghouse services and considers clearinghouse administrative, legal, and technical underpinnings.

## § 5.2 Conventional Clearinghouses and Third-Party Service Providers

In contrast to the envisioned EDI clearinghouse, a conventional or limited-purpose clearinghouse generally is limited to providing specialized services, such as clearing funds or settling accounts. In the banking industry, for example, it is defined as "the place maintained by a group of banks as a center for exchanging checks and drafts drawn against one another, and adjusting balances."<sup>3</sup> An EDI clearinghouse is intended to do much more.

Several factors may also preclude existing third-party service providers (TPSPs), such as value-added networks (VANs), from successfully performing the wide range of general-purpose functions that may be provided by an EDI clearinghouse. First, a TPSP might be perceived as giving preferential treatment to its own customers to the detriment of interconnected

<sup>1</sup> See M. Baum, *EDI and the Law* 136–138 (I. Walden ed. 1989) (brief discussion of EDI clearinghouse legal issues).

<sup>2</sup> "There is a sharp pull between technology's ambition to maximize *uniformity* and the demand of market forces to maximize *diversity*," *Proposed Automated Tariff Filing Initiative, hearing of Federal Maritime Commission* (1990) (testimony of Levy, counsel to North Europe Conferences), reported in Beargie, *Automated Tariff Design Flawed*, Am. Shipper, Dec. 1990, at 73.

<sup>3</sup> Webster's New Twentieth Century Dictionary, Unabridged 336 (2d ed. 1977). The National Automated Clearinghouse Ass'n (NACHA) defines a *clearinghouse* as a "voluntary association of depository institutions that facilitates the clearing of checks or electronic items through the direct exchange of funds between members." Implementing ACH Corporate Payments 157 (NACHA 1987). The UCC defines *clearinghouse* as "any association of banks or other payors regularly clearing items." U.C.C. § 4–104(d). For purposes of U.C.C. § 4 on bank deposits and collections, the term *item* is defined as "any instrument for the payment of money even though it is not negotiable but does not include money". U.C.C. § 4–104(g). With respect to the UCC definition of *clearinghouse*, "[o]ccasionally express companies, governmental agencies and other non-banks deal directly with a clearing house; hence the definition does not limit the term to an association of banks." U.C.C. § 4–104, Official Comment No. 2 (1989).



noncustomers. It may provide to its customers (1) better information, (2) better queuing in first-in-time time-sensitive transactions, and (3) preferential listings on trade databases. Second, a TPSP might not possess resources sufficient to instill user confidence against liability risks.

A TPSP can have various or diverse business relationships with users and vendors, or other TPSPs. In contrast, an EDI clearinghouse must act as an impeccably impartial intermediary (a trusted entity),<sup>4</sup> and therefore should not engage in independent commercial relationships with users, vendors, TPSPs, or other clearinghouses unless such relationships are necessary for proper clearinghouse operations and are publicly disclosed.<sup>5</sup> In order to preserve impartiality and to avoid even the appearance of partiality, a purveyor of goods and services necessary for clearinghouse operations should be precluded from participating in clearinghouse-mediated trading if the purveyor has access to, or knowledge of, clearinghouse security procedures or materials that could compromise such security. Implicit in the mission of the clearinghouse is a duty to act with unwavering integrity and fairness.<sup>6</sup>

Whereas the general mission of an EDI clearinghouse is to provide varied services that facilitate electronic commerce, a TPSP need not offer comparable enhanced services and, by definition, a TPSP need only provide a communications pipeline for trading partner transactions.

Notwithstanding these distinctions between an EDI clearinghouse and a TPSP, there are some similarities. TPSPs have enabled small business to enter the EDI marketplace with little capital investment; they are not even required to purchase EDI translation software. The EDI clearinghouse may similarly aid in equalizing small and large businesses by providing services that are generally too expensive to be developed and implemented by small businesses.<sup>7</sup> To this extent, both clearinghouses and TPSPs are trade facilitation mechanisms.

### § 5.3 Clearinghouse-like Implementations

Before examining EDI clearinghouse services in detail, this chapter examines some of the services offered by existing clearinghouse analogs and

their implications for possible clearinghouse infrastructure. Sections 5.4 through 5.12 describe clearinghouse-like implementations and supporting legal structures in selected industries and sectors and relate these structures to the proposed EDI clearinghouse.

### § 5.4 —Health Care

Baxter Healthcare Corporation<sup>8</sup> created the Analytical Systems Automated Purchasing (ASAP®) system in 1976 for on-line supply ordering. It set a precedent in the strategic use of commercial data systems by offering "free" terminal equipment and data services in conjunction with electronic ordering.<sup>9</sup> In 1987 Baxter introduced a multivendor computer supply system, called ASAP® Express, that simplifies and standardizes access to over 1,500 hospital suppliers through a single system.<sup>10</sup> "ASAP Express is designed to function as a clearinghouse within the health-care industry, offering health-care customers the opportunity to place product orders for multiple vendors through one automated system."<sup>11</sup> It permits customers to order goods from Baxter and its subsidiaries, place orders for products supplied by other vendors, receive order acknowledgments from Baxter and other vendors, inquire on an order's status, and initiate repetitive or standing orders for non-Baxter products.<sup>12</sup>

Customers may order products from Baxter suppliers or other suppliers through the ASAP Express system by sending EDI transactions with the sender's and intended supplier's unique ID numbers in an EDI interchange envelope.<sup>13</sup> Baxter may thereby recognize which transactions are directed to Baxter and which are directed to other suppliers, without becoming

<sup>8</sup> Previously named the American Hospital Supply Company, it was acquired in 1985 by Baxter Travenol Laboratories.

<sup>9</sup> See Harvard Business School Case Study, *Baxter Healthcare Corporation: ASAP Express*, 9-188-080 rev. (Jan. 1989).

<sup>10</sup> This PC-based multivendor service was introduced in conjunction with GE Information Services, following ad hoc focus group discussions with Premier Hospitals Alliance, a group of 37 major voluntary hospitals that buy some \$5 billion worth of health care products annually. Some of Premier's hospitals served as early pilot sites for the ASAP Express system. Between 3,600 and 3,800 hospitals use one of the various family of ASAP services. Letter from Rachel Forester, ASAP Systems/EDI Market Manager, to Michael Baum (Feb. 22, 1991); Thackray, *Baxter International's ASAP Express: New Strategic Thrust Into Hospital Supplier*, IN, Spring, 1988.

<sup>11</sup> Price Waterhouse, *Baxter Healthcare ASAP Express Clearinghouse System Third Party Report 3* (Feb. 10, 1988).

<sup>12</sup> *Id.*

<sup>13</sup> "The interchange header and trailer segments envelope one or more functional groups or interchange-related control segments" to facilitate their communication. X12.5 Interchange Control Structures, X2 Standards, Draft Version 3 Release 1 (Doc. No. ASC X12S/90-850) at 1 (1990). See also Ch. 2.

<sup>4</sup> See § 5.25 on trusted entities within context of public key certification authorities.

<sup>5</sup> This is not intended to suggest that TPSPs do not have an obligation to operate with integrity. The contrary is true.

<sup>6</sup> Compare with obligations of notary public to be disinterested, Ch. 4.

<sup>7</sup> "Large corporations and government agencies need to take steps to accommodate small trading partners that may not necessarily have the money or expertise to implement EDI. . . . [O]therwise, the ability of the U.S.'s nineteen million small businesses to compete for new business could be endangered—resulting in a problem that could have serious impact on the nation's economy." \_\_\_\_\_, *Environment & Labor Subcomm. of the House Small Business Comm.*, 101st Cong., 1st Sess. (Dec. 1989) (statement of Congressman Estaban Torres, subcomm. chairman).

privity to the transactions. That is, Baxter can evaluate each transaction's header for communications purposes and serve as a communications intermediary without reading the content of each message. Notwithstanding ASAP's security measures, those suppliers or customers who fear the central role of Baxter in handling their business communications can also choose to connect directly to each other (that is, customer-to-vendor)<sup>14</sup> and thereby effectively bypass Baxter. Although this direct connection option certainly reduces Baxter's potential for impropriety, it does not directly resolve all confidentiality issues. Encryption could be made available, although corporate culture and other factors have discouraged its use.<sup>15</sup>

Passwords, authorizations, and audit trails are intended to enhance ASAP system reliability. Baxter management recognizes that customer and vendor confidence in the ASAP system's integrity is the linchpin to its success.<sup>16</sup> Consequently, Baxter imposes publicly observable and rigorous controls. For example, customers and vendors alike, upon giving 24-hour notice to the ASAP Express hub, may examine and audit the security system. In addition, Baxter has publicly distributed its internal ASAP system audit report.

**Clearinghouse implications.** The Baxter system demonstrates the acceptability of a commercial multivendor independent ordering system. The open audit policy builds user confidence in its integrity, as do rigorous controls and user options (such as those that permit users to bypass Baxter and to connect directly with other vendors). An EDI clearinghouse should carefully consider the ASAP Express controls regime in providing diverse mechanisms for interconnection, integrity, and privacy.

### § 5.5 —Payment Intermediaries

The Automated Clearing House (ACH) network is the predominant electronic payment system for corporations and consumers in the United States. Significant legal, administrative, and technical structures have been

developed that underlie the network's operation and its participants' expectations for reliability. The National Automated Clearing House Association describes the ACH as:

[A] nationwide electronic payments system used by more than 20,000 participating financial institutions, 100,000 corporations, and millions of consumers. The concept of a nationwide electronic payments network was championed initially in the late sixties by a group of imaginative bankers who recognized the need for an electronic alternative to check payments. In 1974, after the successful development of regional automated clearing house associations in California, Georgia, New England, and the Upper Midwest, the National Automated Clearing House Association ("NACHA") was formed as the regulatory body for the ACH Network. Under the aegis of NACHA, the ACH Network has grown into a national payments system processing more than one and a half billion payments annually and growing by 20% each year. In addition to clearing services, its forty-two regional associations offer marketing, training, publications, and operations support to member depository financial institutions that include commercial banks, savings and loans, credit unions, and mutual savings banks.

The ACH payments mechanism is unique in the wide variety of payment options it offers to both consumers and corporations. Direct deposit, pre-authorized payment, home banking, point of sale, cash concentration and disbursement, corporate trade payments, and check truncation are among the many applications available.<sup>17</sup>

NACHA has developed comprehensive rules prescribing clearinghouse functions and procedures for its members.<sup>18</sup> The Rules and Operations Committee (a NACHA standing committee) is made up of individuals from member associations and depository institutions, regular staff, representatives of the Federal Reserve, and a representative from the Treasury Department. The committee meets three times a year and discusses potential rule changes.<sup>19</sup> NACHA has developed detailed arbitration rules<sup>20</sup> that affect participating depository financial institutions. These rules include procedures for complaint filing and case presentation and appeal. Interestingly,

<sup>14</sup> Via Asynchronous Communications Guidelines developed within ASC X12. Where customer and vendor directly connect and trade, Baxter's role is effectively diminished.

<sup>15</sup> In the absence of clear guidelines concerning confidentiality of EDI communications via communications intermediaries, end-to-end encryption when appropriately implemented can serve an important purpose. See Ch. 7 on privacy and the Electronic Communications Privacy Act of 1986.

<sup>16</sup> The ASAP Express clearinghouse will be used by vendors as long as its integrity is ensured. "It would be suicide [to Baxter and to ASAP Express] if we compromised confidentiality. Our participating vendors and customers know that." Telephone conversation with Rachel Forester, ASAP Systems/EDI Market Manager, Baxter Healthcare Corp. (May 2, 1990).

<sup>17</sup> *Introduction*, 1991 ACH Rules (NACHA 1991). This discussion of NACHA and the ACH is also relevant to the material on EDI payments in Ch. 2.

<sup>18</sup> NACHA members are depository financial institutions, including banks, thrifts, and credit unions.

<sup>19</sup> If the committee approves a rule change, the proposal is sent to the NACHA Executive Committee, which decides whether it should go out for ballot to the NACHA membership. See 1990 ACH Rules, art. 13.1 Amendment of the Rules, OR 47 (NACHA 1991). The discussion of NACHA rules is intended as an example of administrative procedures relevant to various aspects, types, or activities of EDI clearinghouses.

<sup>20</sup> 1991 ACH Rules, art. 11, OR 31-34 (NACHA 1991).



these procedures have yet to be invoked because its members have been successful in informally resolving disputes.<sup>21</sup>

NACHA participates in the ANSI ASC X12 and UN/EDIFACT standards development process and since April 1987 the NACHA rules permit the incorporation of X12 standard formatted messages in NACHA-formatted payments. Additionally, the Federal Reserve Bank Uniform Operating Circular on Automated Clearinghouse Items, if not inconsistent with NACHA rules, either supplements the ACH rules and supersedes NACHA rules in the event of a conflict.<sup>22</sup>

With respect to EDI payments, NACHA adopted a policy on data security in which it recommends that "ACH participants employ data security techniques in accordance with ANSI standards for authentication and key management," that "NACHA will work with ACH operators to implement data security techniques for various media and for exchanges between operators," and that "[o]n an on-going basis, NACHA will stay abreast of new data security techniques and their applicability to the ACH system to ensure a high level of quality and reliability to all users of the ACH."<sup>23</sup>

NACHA rules also address records retention and management issues:

Each Participating DFI [Depository Financial Institution] is required to retain a record of all entries . . . transmitted or received by it from its ACH for a period of *six years* after the date of such transmittal or receipt and shall, at the request of its customer, or of any other Participating DFI or

<sup>21</sup> Dispute resolution mechanisms are of considerable importance to some clearinghouse functions, such as authentication of records held or processed by the clearinghouse. Cf. M. Ben-Or, O. Goldreich, S. Micali, R. Rivest, A Fair Protocol for Signing Contracts, 36 IEEE Transactions on Information Theory no. 1, at 42 (Jan. 1990) (a technology-driven arbitration mechanism that relies on a third party called the "judge" actually a "simple probabilistic algorithm which is intended to be more "inconspicuous" than other third party contract signing arbiters).

<sup>22</sup> 1990 ACH Rules, 1 Uniform Operating Circular § 1 (NACHA 1990). The Federal Reserve Statement of Direction on Electronic Data Interchange (Sept. 15, 1989) provides that:

The current and potential involvement of the banking industry in EDI services is . . . significant. In light of the Federal Reserve's role as a provider of electronic payments services and the linkage between electronic payments and supporting EDI data, the corporate and financial communities have asked the Federal Reserve to state its future direction with respect to EDI, particularly as it relates to the processing of payment related data.

The Federal Reserve will continue to support the exchange of payment related data that are currently accommodated in its ACH and funds transfer services.

The Federal Reserve intends to continue working with the National Automated Clearing House Association, the American National Standards Institute, and other industry groups to address issues and seek solutions to problems or opportunities associated with EDI, the payments system, and future payment formats.

<sup>23</sup> 1991 ACH Rules OR XV (NACHA 1991).

ACH which originated, transmitted or received any such entry, furnish to such person a printout or other reproduction of the pertinent information relating to such entry. A Participating DFI may impose a reasonable charge for furnishing such information.<sup>24</sup>

\* \* \*

Each ACH is required to retain a record of all entries . . . transmitted or received by it from a Participating DFI or another ACH for a period of *one year* after the date of such transmittal or receipt, and shall, at the request of a Participating DFI or any other ACH that originated, transmitted, or received any such entry, furnish to such person a printout or other reproduction of the pertinent information relating to such entry.<sup>25</sup>

**Clearinghouse implications.** NACHA plays a significant EDI role as a payments intermediary. As such, the ACH must satisfy stringent security and audit controls and fulfill rigid regulatory requirements that arguably could satisfy EDI clearinghouse needs. For this reason, and because of the proper role and the initiatives of banks in handling EDI data not directly related to payment, financial institutions, NACHA, and the ACH rules provide a rich framework from which useful clearinghouse structures can be extrapolated.

## § 5.6 —Bank Card Clearing Services

Bank card clearing service providers serve as financial intermediaries between trading partners and play an important role in allocating risk. The major intermediaries in the bank credit card industry are Mastercard and VISA.<sup>26</sup> Bank card clearing service rules and operations deserve close scrutiny because of their potential contribution to, and interrelationship with, a clearinghouse.

Bank credit card systems consist of four fundamental components:

- (1) cardholders who use bank credit cards to purchase goods and services;
- (2) merchants who accept bank credit cards in exchange for goods and services;
- (3) financial institutions (issuer banks) which issue cards to, and contract with, cardholders; and
- (4) financial institutions (merchant banks) which contract with merchants to accept the bank credit card and thereafter manage the bank credit card accounts of these merchant clients.<sup>27</sup>

<sup>24</sup> NACHA, art. 2, Records (NACHA 1991).

<sup>25</sup> NACHA, art. 8.9, Obligations of Automated Clearinghouses, OR 24 (emphasis added) (NACHA 1991).

<sup>26</sup> National Bancard Corp. (NaBANCO) describes itself as the "premier nonbank third party credit clearinghouse." National Bancard Corp. v. VISA U.S.A., Inc., 596 F. Supp. 1231, 1239 n.10 (S.D. Fla. 1984).

<sup>27</sup> *Id.* at 1237.

Bank card intermediaries establish the operating rules that control the operation of the bank card system. In the case of VISA, members can choose whether to transact directly through VISA (utilizing its VISA BASEII computer system), in which case the VISA operating rules apply, or to interchange transactions outside of the VISA automated system, in which case the operating rules of the alternate system apply. The interrelationship of multiple clearing services demands consistent operating rules to ensure the satisfaction of system users' reasonable expectations of the reliability of and the risks associated with their transactions.<sup>28</sup> The costs involved in processing the transaction between the merchant's bank and the customer's bank are typically charged as an interchange fee,<sup>29</sup> as are the costs of automation and the expenses attendant to the stringent procedures developed and administered by the intermediary.

**Clearinghouse implications.** The bank card clearing services industry is highly automated, sophisticated, and regulated. The financial, administrative, and legal relationships among bank card providers, merchants, and users are complex, highly competitive, and of pedagogical and practical value to the development of clearinghouse structures. Moreover, as financial services and EDI payments are expanded and integrated, bank card rules and regulations will need to be accommodated by, and will influence, the clearinghouse.

### § 5.7 —Commercial Aviation

The airline industry's many clearinghouse-like entities, extensive technological resources, and litigious history make it a critical industry within which to consider clearinghouse issues. For example, airlines and accredited agents participate in the Area Settlement Plan (ASP), a clearinghouse that makes payments to the proper airlines and performs related functions.<sup>30</sup> The Airline Reporting Corporation (ARC) provides "a method of approving authorized agency locations for the sale of transportation, and cost effective procedures for processing records and funds of such sales to carrier customers."<sup>31</sup> The ARC functions as a clearinghouse for about 135

airlines and 22,000 travel agencies and includes the ASP for travel agents to report and to remit proceeds to the respective airlines.<sup>32</sup> The Airline Clearinghouse (ACH) performs intercarrier settlement functions regarding sales of airline tickets. The Airline Tariff Publishing Company (ATPCO) serves as a clearinghouse for information regarding airline fares.

Computerized reservation systems (CRSs) are computer and data communication systems used by travel agents and airlines for flight information, flight reservations, and ticket-printing operations. These systems are owned and operated by various major airlines and travel agencies. The largest CRSs are SABRE (American Airlines), Apollo (United Airlines, USAir, and foreign airlines), SystemOne (Continental Airlines), and WORLDSPAN,<sup>33</sup> which is a joint venture of TWA, Northwest, and Delta. WORLDSPAN is the first computer reservations system to be developed and operated independently of its airline owners. Operated out of its Atlanta, Georgia, headquarters, WORLDSPAN represents approximately 21 percent of the United States travel agency marketplace with nearly 13,000 travel agency subscribers. More than 90 percent of all United States airline tickets are purchased through these four systems.<sup>34</sup> For example, SABRE is connected to more than 100,000 devices and 11,000 travel agency locations. It contains flight information for more than 650 airlines and processes more than 10 million reservations monthly.<sup>35</sup>

The ARC has developed rules to govern many aspects of the reservation process and the responsibilities between agents and the ARC. The rules book includes an agent reporting agreement, security rules, an audit and fraud prevention program, and procedures for the prevention of burglary or theft of ARC documents.<sup>36</sup> These rules are a useful resource for the development of clearinghouse rules.

Despite their great benefits, CRSs have encountered considerable legal challenges. For example, CRSs have come under antitrust attack and, in

<sup>28</sup> Issues related to multiple clearinghouses are considered in the context of cross-certification in § 5.25.

<sup>29</sup> For example, in the case of VISA, the "Issuer's Reimbursement Fee" was based upon "a cost-reimbursement methodology developed in conjunction with Authur Anderson and Co. . . ." National Bancard Corp. v. VISA U.S.A., Inc., 596 F. Supp. 1231, 1239 (S.D. Fla. 1984).

<sup>30</sup> See Republic Airlines, Inc. v. Civil Aeronautics Bd., 756 F.2d 1304, 1309 (8th Cir. 1985).

<sup>31</sup> Airline Reporting Corp., ARC Industry Agent's Handbook § 1.0, at 1 (Oct. 1989).

<sup>32</sup> Trans World Airlines, Inc. v. American Coupon Exch., Inc., 682 F. Supp. 1476 (C.D. Cal. 1988).

<sup>33</sup> WORLDSPAN came into existence in Feb. 1990 and is described as a "neutral" CRS. See WORLDSPAN, News Release (Feb. 7, 1990). Given the economic volatility of the airline industry, CRS ownership and structure will continue to change rapidly.

<sup>34</sup> Competitive Enter. Inst. v. United States Dep't of Transp., 856 F.2d 1563, 1564 (D.C. Cir. 1988).

<sup>35</sup> See *In re Air Passenger Computer Reservation Sys. Antitrust Litig.*, 694 F. Supp. 1443, 1449 (C.D. Cal. 1988). See also Civil Aeronautics Bd. (C.A.B.) final rule, 14 C.F.R. § 255.4(b) (1988), requiring that CRS generate displays based on "neutral" characteristics. American has proposed linking its SABRE system to the largest European reservation system, Amadeus Global Travel Distribution system (Scandinavia Airlines, Lufthansa, Air France, and Iberia), which would give it a network of 126,000 reservation terminals.

<sup>36</sup> Republic Airlines, Inc. v. Civil Aeronautics Bd., 756 F.2d 1304 (\_\_\_\_\_, Cir. 1985). See generally Airline Reporting Corp., ARC Industry Agent's Handbook (Oct. 1989).



some instances, have been found to be illegally biased in favor of a host airline:

When consumers attempt to purchase a ticket on the best available flight their final decision is not solely based upon the merits of the particular flight (flight time, price, service, etc.). Rather, biasing artificially inflates the value of the host airline's flights by listing their flights above better flights. . . . It is unreasonable and therefore an unwarranted competitive advantage because it inhibits competition on the merits.<sup>37</sup>

In a lawsuit brought in 1984 by various airlines alleging high fees and bias in the CRS business, the plaintiffs were not able to demonstrate that United and American Airlines illegally monopolized CRSs, although together United and American constituted approximately 70 percent of the CRS industry. The judge also ruled that the fees charged were not a relevant factor in deciding whether the defendants were monopolizing the CRS industry.

The alleged use of shared databases to affect airline ticket prices among airlines suggests the potential for anticompetitive practices—practices that could also manifest themselves in clearinghouse activities. Fare changes and airline coding procedures are claimed to contain signals to other airlines through which the airlines may attempt to collusively set prices, send warnings about other airlines' prices, or even test the waters by preannouncing fares.<sup>38</sup>

EDI may open a new frontier for such intercompany signalling. EDI utilizes extensive common data and segment dictionaries that contain thousands of codes, many of which are developed by specific industries and used in conjunction with private conventions.

**Clearinghouse implications.** The airline and CRS industries are pioneers in introducing sophisticated electronic databases and networks for interenterprise electronic commerce within a highly competitive environment. In this undertaking, they have encountered considerable legal challenges. The EDI clearinghouse may avoid similar problems by ensuring that its systems are operated fairly, do not serve as a vehicle for price fixing, are structured such that they do not discriminate against competitors or certain industry members, and do not require unreasonable fees or terms for service commencement, use, or termination.

<sup>37</sup> *In re Air Passenger Computer Reservation Sys. Antitrust Litig.*, 694 F. Supp. 1443, 1474 (C.D. Cal. 1988). Renewed Congressional and Dep't of Transp. efforts to require nonbiased systems are underway.

<sup>38</sup> Nomani, *Fire Game: Airlines May Be Using a Price-Data Network to Lessen Competition*, Wall St. J., June 28, 1990, at 1. John Timmons, minority counsel of the Senate Aviation Subcommittee, has commented that "[t]he information age has redefined antitrust. We don't need Mr. Smith to call Mr. Jones." *Id.*

### § 5.8 —Defense Department's Electronic Commerce and Treasury Department's Vendor Express

Two government electronic programs exhibit interesting features relevant to the EDI clearinghouse: the Electronic Commerce project, administered by the Department of Defense Electronic Commerce Program Office, and the Vendor Express program, administered by the Treasury Department's Financial Management Service.

The Electronic Commerce program is an ambitious project to automate government solicitations, purchasing, and payment.

The [Electronic Commerce] design calls for an electronic bulletin board system that would broadcast low-dollar solicitations and help businesses nationwide to gain access to the solicitations via third-party value-added networks. The bulletin board requires installing EDI software in the approximately 2,500 procurement offices of the federal government nationwide. These offices would originate electronic request-for-quote [transaction sets] and send them via a government data network to a central repository/bulletin board. The repository, in turn, would be downloaded daily (or more frequently) to the major EDI value-added networks. Small business, using low-end EDI software running on a PC, would dial their respective networks and query the bulletin board. A software program or perhaps a menu system would help the small-business vendor to locate just those solicitations that are relevant.<sup>39</sup>

The Electronic Commerce pilot program is expected to be fully operational in fiscal 1992.<sup>40</sup>

Since July 1987, Treasury's Financial Management Service (FMS) has operated the Vendor Express program, an electronic funds transfer mechanism for making vendor and miscellaneous payments. Payees include companies, state and local governments, and other organizations doing business with the federal government. With Vendor Express, value transfer and remittance information move together electronically through the banking system.<sup>41</sup> Vendor Express is a key EDI component for government payments.

The electronic transmission of payment instructions is communicated from federal agency certifying officers to FMS disbursing officers. The FMS Electronic Certification System replaces manual systems "for voucher

<sup>39</sup> *Federal Electronic Commerce Program Factors Small-Business EDI Use*, 6 INPUT EDI Reporter 3, at 8-10 (March 1991).

<sup>40</sup> Telephone conversation with Dana Ellingen, Asst. Project Leader, Electronic Commerce Project, Lawrence Livermore National Laboratory (Apr. 23, 1991).

<sup>41</sup> Using automated clearinghouse formats such as CCD+ and CTX. Remittance information accompanying the payment is structured in the ANSI X12.4 convention. See Ch. 2 on TPA electronic payments issues.

preparation, certification, transmission, and verification."<sup>42</sup> It "provides positive identification of the certifying officer who authorizes<sup>43</sup> the voucher and ensures the authenticity of the transmitted data." FMS security implementations utilize symmetric key cryptography (DES) and incorporate both ANSI X9.17 and ANSI X9.9 protocols (bank security standards). It also requires trusted software. As a government entity, FMS operates under FIPS PUB 140, the Government Open Systems Interconnect Profile (GOSIP),<sup>44</sup> and Treasury certification procedures for electronic funds transfer devices. Authentication of electronic funds transfer (EFT) payments is based on Treasury Order 106-09 and the Federal Manager's Financial Integrity Act<sup>45</sup> and has been approved by the General Accounting Office.<sup>46</sup>

**Clearinghouse implications.** The Electronic Commerce program represents the first viable government effort to coordinate the EDI community into a ubiquitous multivendor system. It gives considerable attention not only to EDI technology, but to EDI's administrative, security, legal, and payments aspects and practices. This project promises to serve as a catalyst to mature EDI into the primary vehicle for commerce.

Because it bears responsibility for making government payments, Treasury wields great influence and authority over government electronic payments security procedures. Consequently, Treasury's security product certification service<sup>47</sup> procedures for authentication of electronic funds transfers could provide guidance for appropriate EDI clearinghouse security procedures and structures. Treasury regulations contain a plethora of knowledge concerning electronic payment integrity issues, which are relevant to commercial electronic trading and clearinghouse purposes.

## § 5.9 —Securities Trading

Clearinghouses are used in United States securities markets to handle *clearing* (confirming "identity and quantity of the financial instrument or contract being bought or sold, the transaction price and date, and the identity

<sup>42</sup> Fact sheet, Electronic Certification (Financial Management Servs. Aug. 1990).

<sup>43</sup> *Id.*

<sup>44</sup> See Ch. 4 on GOSIP.

<sup>45</sup> P.L. 97-255, 96 Stat. 643 (Sept. 8, 1982).

<sup>46</sup> In satisfaction of requirements in 31 U.S.C. §§ 3325, 3528 (1988).

<sup>47</sup> Criteria and Procedures for Testing, Evaluating and Certifying Message Authentication Devices for Federal EFT Use (2d ed. Sept. 1, 1986). See generally, §§ 5.31-5.36 on testing issues.

of the buyer and seller")<sup>48</sup> and *depositories* (holding "stocks and bonds for safekeeping on behalf of their owners").<sup>49</sup> The major goals for such clearinghouses are risk reduction, efficiency, and safety.<sup>50</sup> "Clearinghouses provide the buyer with a guarantee that [he or she] will receive the securities—or other interest—[he or she] purchased, and provide the seller with a guarantee that [he or she] will receive payment."<sup>51</sup>

Section 17A of the Securities Exchange Act Amendments of 1975 mandates a national clearing and settlement system "for the prompt and accurate clearance of settlement of transactions in securities . . . [with] due regard for the public interest, the protection of investors, the safeguarding of securities and funds, and maintenance of fair competition among brokers and dealers, clearing agencies, and transfer agents."<sup>52</sup> As a result, the National Securities Clearing Corporation (NSCC) was established and now clears approximately 95 percent of equity securities.<sup>53</sup>

Securities exchanges have developed various technologies to support their mission, which includes bringing information resources and trading closer to the trading public. For example, the American Stock Exchange, the Chicago Board of Options Exchange, the New York Stock Exchange, the Pacific Stock Exchange, and the Philadelphia Stock Exchange have undergone a change in trading rules to facilitate the electronic linkage of these exchanges. Significant securities automation developments are also underway internationally.<sup>54</sup> Major efforts are currently being made to completely

<sup>48</sup> Office of Technology Assessment (OTA), *Electronic Bulls and Bears, U.S. Securities Markets and Information Technology*, OTA—CIT—469, at 107 (Sept. 1990) [hereinafter *Electronic Bulls and Bears*].

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

<sup>53</sup> *Id.* at 181.

All payments to NSCC are on a net basis; i.e., the NSCC calculates each clearing member's total credit and debit positions and nets to a single figure that is either owed to NSCC or is owed by NSCC. Payment to NSCC is by certified check. Funds are concentrated in one central clearing bank. If a certified check is not received on the settlement date, then payment via Fedwire is required the next morning. NSCC pays selling members with regular bank checks, but intends to move towards the increased use of electronic payments as one way to improve the settlement process.

*Id.* at 187.

<sup>54</sup> For example, the European Price and Information Project (PIPE) will disseminate regulated share price and company information among Europe's 12 stock exchanges and is predicted to become the foundation for a pan-European trading system. The Federation of Stock Exchanges intends to develop more uniform practices among PIPE members. *European Stock Exchange Plan Network*, Comms. Week, Jan. 15, 1990, at 12.



reform the clearance and settlement of securities transactions. This effort is being led internationally by the Group of 30 industrial nations. A special international working committee of the Group of 30 has promulgated nine recommendations to standardize securities clearance and settlement procedures in cross-border equity transactions by 1992 in order to remove the limitations of current trading practices. Group of 30 recommendations of particular relevance to the EDI clearinghouse include: (a) universal conversion from a payment system based on next-day clearinghouse funds to a same-day-funds convention for money settlement of securities transactions; (b) an effective and fully developed central securities depository; and (c) the universal application by 1992 of the standards of securities messages developed by the International Organization for Standardization.<sup>55</sup> C. Richard Justice in his presentation acknowledged the need for "extensive educational efforts by leading industry organizations as well as a significant amount of legal and operational research. Other concepts such as custody and record keeping of investments would have to be dealt with for investors who do not wish to have their existing certificates with a financial intermediary."<sup>56</sup>

Additionally, new and unconventional electronic securities markets are being introduced to eliminate the need for traditional brokerage houses and to permit investors to interact directly through clearinghouses.<sup>57</sup> However, privacy concerns have affected the success of such systems.<sup>58</sup>

<sup>55</sup> ISO Standard 7775, Presentation by C. Richard Justice to Int'l Councils of Securities Dealers and Self Regulatory Ass'ns (Apr. 9-10, 1990).

<sup>56</sup> *Id.* Compare discussions of custody and record keeping in the context of electronic bill of lading systems, Chs. 4 & 11, § 5.11.

<sup>57</sup> "[T]he nations first electronic auction exchange, setting prices off the big board" will permit "investors to submit their buy and sell orders. Then, three times a week, the computer will sort through the orders, come up with a price, and execute trades." Wayne, *A Rock Climber's Reach for the Top on Wall St.*, Wall St. J., Jan. 24, 1991, at D1. CapitaLink Bond Auctions, Inc., provides a network that allows corporate issuers to auction new offerings of registered notes and bonds directly to institutional investors. However, the CapitaLink electronic auction and other systems, which trade privately placed securities sponsored by the National Ass'n of Securities Dealers, are considered to have floundered. "Analysts say issuers and investors in that market prefer to arrange their transactions privately, without being displayed for others to see." Quint, *Electronic Bond Auction Flounders*, N.Y. Times, Nov. 30, 1990, at D5 (emphasis added).

<sup>58</sup> This privacy concern mirrors the concerns of other securities clearinghouse entities with respect to the impact on competitiveness. For example, the Options Clearinghouse Corp. (OCC), which clears and settles options trades between securities option exchanges, expressed concern about the sharing of information with other intermediaries. Letter from OCC to OTA, Feb. 5, 1990.

The OCC points out that the repository for shared information, if it is a market participant having vested interests, possesses data that might enable it to protect itself against loss earlier than others who depend on it for information dissemination. This raises the question of whether a disinterested, independent entity, such

In a commodities market, trading is undertaken by exchanges that have diverse responsibilities, including maintaining "detailed records, and perform[ing] a clearing function to discharge the offsetting contracts that the short or long speculators have no desire to perform."<sup>59</sup> It is a highly regulated activity.<sup>60</sup> Its primary regulatory authorization, the Commodities Exchange Act, prescribes many legal and structural requirements, including that every contract market provide an arbitration procedure for the settlement of traders' claims of no more than \$15,000.<sup>61</sup>

**Clearinghouse implications.** The securities trading arena is an early user of electronic trade facilities and clearinghouses. The globalization of securities trading will further accelerate electronic practices. The securities industry's extensive regulatory environment coupled with advanced computerization and use of intermediaries provides useful lessons for an EDI clearinghouse.

## § 5.10 — Floral Delivery

Three major floral clearinghouses (FCs) facilitate the long-distance purchase, delivery, and settlement of flower orders: American Floral Services (AFS), Florist's Transworld Delivery Association (FTD), and Teleflora.<sup>62</sup> FC services include:

- (i) clearinghouse-banking functions, insuring the reliable flow of money between florists who may otherwise be strangers;

---

as a Federal regulator or a private contractor, would be preferable as the system operator. The NSCC notes concern for BOTCC access to confidential information and raises the question of whether futures clearing organizations may misinterpret pay/collect data and take inappropriate action based on it.

Electronic Bulls and Bears, at 114. See also Eichenwald, *Wall Street's Cutbacks Sidestep Fat Budgets for High-Tech Trading*, N.Y. Times, Apr. 7, 1991, at 8f, Cols. A-E.

<sup>59</sup> *Merrill Lynch, Pierce, Fenner & Smith v. Curran*, 456 U.S. 353, 102 S. Ct. 1825, 1829 (1982).

<sup>60</sup> Commodity Exchange Act (CEA), 7 U.S.C. § 1 et seq. (1976 & Supp. IV). Six major legislative enactments preceded the CEA and are succinctly described in *Merrill Lynch, Pierce, Fenner & Smith v. Curran*, 456 U.S. 353, 102 S. Ct. 1825, 1825 (1982).

<sup>61</sup> CEA § 5a(11); § 209 of the 1974 amends, 88 Stat. 1401 (adding § 5a(11) of the CEA, codified as subsequently amended, 7 U.S.C. § 7a(ii) (1976 Supp. IV)). Arbitration mechanisms undertaken by clearinghouses should be evaluated for application to EDI clearinghouses.

<sup>62</sup> There are approximately 31,000 floral shops in the United States with average gross sales in 1984 of \$185,000. Annual florist business totalled \$5-6 billion, and some \$750 million, or 12-15%, of that was in long-distance flower delivery. American Floral Serv. v. Florists' Transworld Delivery, 663 F. Supp. 201, 204-205 (N.D. Ill. 1986).

- (ii) communications, including both provision of private on-line systems and publication of directories identifying distant florists with whom to communicate;
- (iii) advertising, including . . . general promotion of the idea of sending flowers long-distance;
- (iv) quality control, through both published standards and test orders; and
- (v) education, through publications and seminars for florists and floral designers.<sup>63</sup>

By law, floral shops are permitted membership in and the use of more than one FC. "Any attempt by any wire organization to enforce exclusive use of their particular clearing facility constitutes a *per se* illegal boycott under Section 1 of the Sherman Act."<sup>64</sup> Each FC establishes a set of rules and regulations governing its use. These rules and regulations, which create "restrictions between one level of an industry and another are 'vertical' . . . [and] are typically subject to rule-of-reason analysis."<sup>65</sup> Such FC rules and regulations are considered *pirate-order rules*, which are defined as "legitimate agreements ancillary to cooperative agreements between florists and clearinghouses and, as such, are valid under rule-of-reason analysis where there was no barrier to entry that prevented competition."<sup>66</sup>

**Clearinghouse implications.** The structure of the FCs, which provide a broad set of services, could, in part, be emulated by an EDI clearinghouse. The major legal issues raised by the FCs have concerned restraint of trade. These issues illuminate potential clearinghouse problems, particularly in markets that can economically support only a few competitor clearinghouses.

### § 5.11 —Documentary Transfers

Efforts to electronically transfer title to goods have been underway for more than a decade. Prior efforts<sup>67</sup> have failed to gain sufficient support, due to confidentiality concerns and a lack of confidence that an electronic system could provide enforceable attributes of negotiability.<sup>68</sup> *Negotiability*

<sup>63</sup> *Id.* at 204.

<sup>64</sup> *Id.* at 209. See generally Ch. 10.

<sup>65</sup> *Id.* at 218–19.

<sup>66</sup> *Id.* at 202 n.9.

<sup>67</sup> See Ch. 11 (negotiability and bills of lading; relevant EDI document issues).

<sup>68</sup> Bills of lading, even in conventional paper-based media, have been recognized as easy to fake. "A bill of lading showing ownership of \$16 million in cargo is easy enough to obtain or forge . . . especially in contrast with such instruments as stock certificates

has been defined as the ability to transfer "an instrument in such form that the transferee becomes a holder [in due course]."<sup>69</sup> In the regular course of business, a document of title, such as a bill of lading, "is treated as adequately evidencing that the person in possession of it is entitled to receive, hold and dispose of the documents and the goods it covers."<sup>70</sup> Rights accruing to the recipient of a negotiable document include title to the documents and title to the specified goods.<sup>71</sup>

No international convention or agreement adequately addresses the legal aspects of electronic title to goods, although interest in such an undertaking is accelerating.<sup>72</sup> Efforts to resolve the electronic negotiability issue are discussed in Chapter 11.

The Comité Maritime International (CMI) Rules for Electronic Bills of Lading<sup>73</sup> have been developed to provide a mechanism for electronically negotiating documents of title and to overcome prior legal problems in the electronic transfer of title. The system is structured so that specified data will be considered *prima facie* evidence of ownership. The key provisions of these rules specify the manner in which the electronic transfer of title is to occur:

A transfer of the Right of Control and Transfer shall be effected:

- (i) by notification of the current Holder to the carrier of its intention to transfer its Right of Control and Transfer to a proposed new Holder, and
- (ii) Confirmation by the carrier of such notification message; whereupon
- (iii) the carrier shall transmit the information as referred to in Article 4 (except for the Private Key) to the proposed new Holder; whereafter

or bonds, which are intricately engraved so as to be hard to counterfeit." *Shipping Document Fraud Rising*, Am. Shipper, (Feb. 1990, at 96 (Comments of John Kelly, commanding officer of Special Frauds Squad, New York City Police Dep't).) Another issue that has been raised as an impediment to electronic negotiability is the difficulty of achieving electronic document uniqueness, because all electronic representations are copies. See generally D. Chaum, *Privacy Protected Payments Unconditional Payer and/or Payee Untraceability*, Smart Card 2000 (D. Chaum & I. Schaumüller-Bichl eds. 1989).

<sup>69</sup> U.C.C. § 3-202 (within the context of commercial paper).

<sup>70</sup> U.C.C. § 1-201(15).

<sup>71</sup> U.C.C. § 7-502.

<sup>72</sup> Neither the U.N. Convention on Contracts for the International Sale of Goods of 1980 nor the International Chamber of Commerce's *Incoterms 1990* (ICC Pub. No. 460) resolve the negotiability issue. See H. Thomsen & B. Wheble, *Trading with EDI, The Legal Issues* 185 (IBC 1989).

<sup>73</sup> Developed by the Subcommittee on Electronic Transfer of Rights to Goods in Transit, Contracts of Carriage, Comité Maritime International. As adopted, June 30, 1990, in Paris [hereinafter Rules]. See App. D.



(iv) the proposed new Holder shall advise the carrier of its acceptance of the Right of Control and Transfer; whereupon

(v) the carrier shall cancel the current Private Key and issue a new Private Key to the new Holder.

The transfer of the Right of Control and Transfer in the manner described above shall have the same effect as the transfer of such rights under a paper bill of lading.<sup>74</sup>

The rules define a *private key*<sup>75</sup> as:

any technically appropriate form, such as a combination of numbers and/or letters, which the parties may agree for securing the authenticity and integrity of a Transmission. . . . The Private Key is unique to each successive Holder. It is not transferable by the Holder. The carrier and the Holder shall each maintain the security of the Private Key. . . . The carrier shall only be obligated to send a Confirmation of an electronic message to the last Holder to whom it issued a Private Key, when such Holder secures the Transmission containing such electronic message by the use of the Private Key. . . . The Private Key must be separate and distinct from any means used to identify the Contract of Carriage, and any security password or identification used to access the computer network.<sup>76</sup>

SEADOCS, a prior effort by the Chase Manhattan Bank and INTER-TANKO to automate trade documentation, included a central registry that authenticated its transactions as follows:

(i) each party's message must be confirmed by at least one or more other messages, (ii) messages are re-filed to the presumed sender and must be re-acknowledged, and (iii) each message has a header code which is unique to sender and message as it must contain an element from the prior sender and from the computer acknowledgement message.<sup>77</sup>

Ancillary to automating documents of title, the creation of clearinghouse-like entities for central booking in the shipping industry has been proposed or attempted. One such endeavor is EDISHIP, "a unique, jointly

<sup>74</sup> Rules §§ 7.b, 7.d.

<sup>75</sup> Because the term *private key* generally is recognized as a term of art most often used in the context of an asymmetric cryptosystem, it might have been preferable for this provision to have employed the term *secret key*, which is generally understood to imply a symmetric cryptosystem. See Ch. 4.

<sup>76</sup> Rules §§ 2.f, 8.a, 8.b, 8.c.

<sup>77</sup> See Urbach, *The Electronic Presentation and Transfer of Shipping Documents*, Electronic Banking—The Legal Implications 111 (Goode ed. 1985). Reed, *Authenticating Electronic Mail Messages—Some Evidential Problems*, The Modern Law Review (Sept. 1989) at 655.

funded software sharing agreement . . . which could be considered a fore-runner for central booking."<sup>78</sup>

**Clearinghouse implications.** The problems associated with the electronic negotiation of documents present some of the most difficult challenges to electronic commerce. The CMI rules constitute an innovative framework designed to facilitate the transfer of negotiable documents of title. Although it remains unclear whether the rules will achieve widespread adoption or legal standing, they provide an important contribution to efforts to transfer title electronically and serve as an example of technical/legal rules relevant to the EDI clearinghouse.

## § 5.12 —UCC Security Interest Filings

This section examines U.C.C. article 9 (Secured Transactions; Sale of Accounts and Chattel Paper), which provides detailed filing procedures that may prove helpful in evaluating clearinghouse structures, particularly when the clearinghouse serves a governmental instrumentality.

Article 9 provides a system for the creation of *security interests*. A security interest is "an interest in personal property or fixtures which secures payment or performance of an obligation."<sup>79</sup> Security interests attach by (1) putting the collateral in the possession of the secured party pursuant to agreement, (2) giving value, (3) the debtor acquiring rights in the collateral, and (4) executing a security agreement.<sup>80</sup>

Execution of a financing statement generally is required to perfect a security interest.<sup>81</sup> A financing statement is a writing that "gives the names of the debtor and the secured party, is signed by the debtor, gives the [parties'] address[es] . . . and contains a statement . . . describing the . . . collateral."<sup>82</sup>

<sup>78</sup> Canna, *Central Booking—Is It the Solution?*, Am. Shipper, May 1990, at 12. The missions of EDISHIP include "creating a cooperative business environment" and "working towards recommending one single EDI standard, one message format, one third-party network and one software product." *Id.* at 14. However, concern about centralized booking creates an artificial barrier to such electronic trade, and other concerns persist. *Id.*

<sup>79</sup> U.C.C. § 1-201(37).

<sup>80</sup> U.C.C. § 9-203. See J. White & R. Summers, Uniform Commercial Code, § 23-2, at 786 (1972).

<sup>81</sup> There are various exceptions to the requirement of a financing statement; for example, none is required when the security interest in collateral is in possession of the secured party. U.C.C. § 9-302(1). An instrument "is said to become perfect when recorded (or registered) or filed for record, because it then becomes as good to all the world." Black's Law Dictionary 1296 (Rev. 4th ed. 1968). See U.C.C. § 9-302 (when filing is required to perfect security interest); U.C.C. §§ 9-401–9-408 (filing).

<sup>82</sup> U.C.C. § 9-402(1).

### Notice

*Notice*, rather than a full *record copy* of the underlying security agreement is filed. "The notice itself indicates merely that the secured party who has filed may have a security interest in the collateral described. Further inquiry of the parties concerned will be necessary to disclose the complete state of affairs."<sup>83</sup>

**Relevance to the clearinghouse.** In connection with its provision of clearinghouse contract-enforceability services,<sup>84</sup> a clearinghouse could store either a record copy of the transaction or a transaction summary (for example, a digest of the message). Upon trading partner request, the clearinghouse could also store a copy of underlying trade agreement(s) (such as TPAs and underlying terms and conditions agreements).

### Place of Filing

Both [local and state] systems have their advocates and both their own advantages and drawbacks. The principal advantage of state-wide filing is ease of access to the credit information which the files exist to provide. Consider for example the national distributor who wishes to have current information about the credit standing of the thousands of persons he sells to on credit. The more completely the files are centralized on a state-wide basis, the easier and cheaper it becomes to procure credit information; the more the files are scattered in local filing units, the more burdensome and costly. On the other hand, it can be said that most credit inquiries about local businesses, farmers and consumers come from local sources; convenience is served by having files locally available and there is not great advantage in centralized filing.<sup>85</sup>

**Relevance to the clearinghouse.** Centralized or decentralized clearinghouse architectures can provide different levels of accessibility, service, and cost. The parties may desire to prevent transactions from entering interstate commerce for legal, economic, security, and regulatory reasons.<sup>86</sup> Reliable, efficient, and secure distributed networks may overcome the place-of-filing concerns raised in UCC commentary, because the clearinghouse (as a modern database) need no longer be centralized to provide ease of use and to ensure adequate controls.

<sup>83</sup> U.C.C. § 9-402, Official Comment 2 (emphasis added). Record copy is a brief summary rather than the complete security agreement.

<sup>84</sup> See § 5.14 on clearinghouse enforceability services.

<sup>85</sup> U.C.C. § 9-401, Official Comment 1. See § 5.16 (clearinghouse structure).

<sup>86</sup> For example, to keep the clearinghouse and its transactions within a local access and transport area (LATA).

### Erroneous Filings

The UCC adopts a *good faith* standard concerning insufficient filings:

Where a secured party has in good faith attempted to comply with the filing requirements but has not done so correctly . . . , [it is] effective in so far as it was proper, and also makes it good . . . against any person who actually knows the contents of the improperly filed statement. The subsection rejects the occasional decisions that an improperly filed record is ineffective to give notice even to a person who knows of it.<sup>87</sup>

**Relevance to the clearinghouse.** Erroneous-filing-type issues could arise by: (1) sending transactions to the wrong clearinghouse(s), (2) providing incomplete, expired, or incorrect addresses or security credentials to the messaging system/clearinghouse, (3) following the wrong rules or procedures, or (4) otherwise failing to comply with clearinghouse procedures. Because reliability and certainty are critical to the clearinghouse, the UCC's lenient approach, reflected in a good-faith standard, should not be adopted by a clearinghouse unless specific business requirements and fairness dictate otherwise. Technology can assist in providing acknowledgments of filings/transactions in a user-friendly manner as well as in increasing clearinghouse reliability, such that implementation of a stricter standard for erroneous clearinghouse filings would not prove unreasonable.<sup>88</sup>

### Formal Requisites for a Filing

U.C.C. article 9-402 delineates a formal financing statement filing process, and includes a suggested model filing form.

**Relevance to the clearinghouse.** Clearinghouse(s), industry association(s), and/or standards bodies could develop model electronic filing documents for record copy or notice purposes or use existing or extensions to existing

<sup>87</sup> U.C.C. § 9-401, Official Comment 5. U.C.C. § 9-402(8) provides: "A financing statement substantially complying with the requirements of this section is effective even though it contains minor errors which are not seriously misleading." Cf. U.C.C. § 9-402, which provides for "minor errors which are not seriously misleading"; and U.C.C. § 2-207(2)(b) which addresses terms that "materially alter" an acceptance. In both cases, potential for conflict and varying interpretation may impede clearinghouse certainty.

<sup>88</sup> Note that one state's UCC filing office returns 10 to 20 filings per day that are noncompliant with the filing statute, including: documents filed in the wrong jurisdiction, unsigned checks, unsigned documents, and continuation statements filing in the wrong jurisdiction. Telephone conversation with Joseph Sheehan, Mass. Secretary of State's UCC Office (Mar. 8, 1991).



standards.<sup>89</sup> The clearinghouse should be sufficiently flexible to process varied forms.<sup>90</sup>

### Witnesses and Acknowledged Filings

The UCC has eliminated many of the formal requisites of Financing Statements:

This section departs from the requirements of many precode . . . statutes that the instrument filed be . . . acknowledged or witnessed or accompanied by affidavits of good faith. Those requirements did not seem to have been successful as a deterrent to fraud; their principal effect was to penalize good faith mortgagees who had inadvertently failed to comply with the statutory niceties. They are here abandoned in the interest of a simplified and workable filing system.<sup>91</sup>

**Relevance to the clearinghouse.** This UCC policy of simplification is relevant to the clearinghouse particularly because it is not practical to require the personal presence of the filer. However, requirements for obtaining electronic security credentials from a clearinghouse may warrant personal presence (such credentials could be used for multiple transactions).

### Filing Receipts

U.C.C. § 9-403(1) provides that "[p]resentation for filing of a financing statement and tender of the filing fee or acceptance of the statement by the filing officer constitutes filing under this Article." Common filing practices provide for tender of a receipt to the filer upon presentation of the financing statement and filing fee.<sup>92</sup> Moreover:

[A] filing officer shall mark each statement with a file number and with the date and hour of filing and shall hold the statement or a microfilm or other photographic copy thereof for public inspection. In addition the filing officer shall index the statement according to the name of the debtor and shall note in the index the file number and the address of the debtor given in the statement.<sup>93</sup>

**Relevance to the clearinghouse.** Acknowledgments and receipts are important components of clearinghouse functions, particularly upon the filing of a record copy, message authentication code, or transaction digest. Although an EDI functional acknowledgment could acknowledge receipt, stronger acknowledgment mechanisms can be implemented.<sup>94</sup>

### Duration of Filing and Termination

U.C.C. § 9-403(2) states that a "filed financing statement is effective for a period of five years from the date of filing. The effectiveness of the filed financing statement lapses on the expiration of the five year period unless a continuation statement is filed prior to the lapse" (because publicly filed financing statements are self-clearing).

**Relevance to the clearinghouse.** In its record-keeping role, duration of filing and termination issues are important to a clearinghouse in determining and properly acting upon expiration period(s) for acknowledgments, logs, record copy filings, or other retained data. A record copy could be marked by the filer with an expiration date to indicate when a record is to be deleted by a clearinghouse, which could then charge the filer a fee according to the requested retention period, the level of security to be applied, and other factors. The disposal of clearinghouse records must also be carefully and explicitly undertaken.

U.C.C. § 9-404(2) provides that:

If the filing officer has a microfilm or other photographic record of the financing statement, and of any related continuation statement . . . he may remove the originals from the files at any time after receipt of the termination statement, or if he has no such record, he may remove them from the files at any time after one year after receipt of the termination statement.<sup>95</sup>

<sup>89</sup> In the form of new EDI transaction sets, messages or specific additional data segments, elements, and codes.

<sup>90</sup> It might also provide on-line interactive filing facilities.

<sup>91</sup> U.C.C. § 9-402, Official Comment 3. See Ch. 4 on automation of the notarial process.

<sup>92</sup> Art. 9 also provides an optional facility for delivering a time/date stamped copy of the financing statement and a certificate of filing. U.C.C. § 9-407(1).

<sup>93</sup> U.C.C. § 9-403(4).

<sup>94</sup> See Ch. 4 concerning the interconnect mailbag and *P<sub>edi</sub>* acknowledgments. When public key cryptography is used, the bilateral exchange of acknowledgments can provide strong assurances of data integrity and authenticity. However, as noted in § 5.24, to the extent that digitally signed communications are virtually unforgeable, the value of an intermediate record keeper is minimized (depending on how it was implemented), except for security credential (such as for the creation; promulgation; and revocation of certificates) and the time-stamping purposes. See Ch. 4 concerning time stamping applications of intermediate record keepers.

<sup>95</sup> The UCC "provides a permissive device for noting of record any release of collateral" that does not require a separate filing, "so that fewer inquiries will have to be made by persons who consult the files." U.C.C. § 9-406, Official Comment.

A related clearinghouse issue concerns whether a filed record copy should be appended to an electronic statement of termination or should, rather, be deleted upon termination.

**Clearinghouse implications.** The UCC provides a detailed treatment of issues and considerations (albeit nonelectronic) relevant to the EDI clearinghouse. Article 9 "sets out a comprehensive scheme" and recognizes the need for "a simple and unified structure within which the immense variety of present-day . . . transactions can go forward with less cost and with greater certainty."<sup>96</sup> A parallel formulation of some clearinghouse structures and goals would appear appropriate and useful to clearinghouse development.<sup>97</sup>

### § 5.13 Clearinghouse Services

Clearinghouse services provide a number of interrelated functions, such as:

1. Reliability and enforceability protections
2. Information repositories, including for security credential, diverse commercial database, and directory services
3. Facilitation of contract formation and tracking
4. Facilitation of system implementation and operation through the propagation of rules and standards and through interconnection services.

It is not contemplated that each trading partner will utilize all available clearinghouse services, nor can any one clearinghouse provide all possible services. Instead, some clearinghouses could be designed to serve particular industries or classes of trading partners. The specific services provided by a

<sup>96</sup> U.C.C. § 9-101, Official Comment.

<sup>97</sup> Recent efforts have been undertaken to computerize UCC filing systems, most notably, in Canada and Iowa. For example, in British Columbia, registrations and searches are available over dial-up links, although use of this system requires prepayment for registration and searches. R. C. C. Cuming, *Computerization of Personal Property Security Registries: What the Canadian Experience Presages for the United States*, 23 U.C.C. L.J. 331, at 338 (1991).

The State of Iowa has recently adopted the first set of comprehensive rules (r. 721-6, Electronic Filing of Documents, Iowa Admin. Code) to permit electronic filing and indexing. See B. Clark & B. B. Clark, *Latest Technology Used by UCC Filing Offices*, 7 Secured Lending Alert No. 1, at 3 (Warren, Gorham & Lamont, Inc. Mar. 1991) (reporting on the initial findings of a U.C.C. art. 9 task force, A.B.A. Sec. of Bus. L.).

clearinghouse will depend on the particular trading community's needs, which, in turn, may derive from many factors, such as:

1. **The particular markets within which trading is effected.** Different markets have varying requirements.
2. **The regulatory and legal requirements of particular markets or businesses.** For example, industries may have various environmental or safety-related reporting regulatory requirements, such as for the communication of material safety data sheets, and varying labor-related requirements, such as for the communication of certifications of compliance with child labor laws.
3. **Trading partner sophistication and technical resources.** Some industries, such as the automobile industry, are relatively highly automated and will implement trading mechanisms of greater complexity than less automated entities.
4. **The nature of the trading relationship.** Trading partners who enjoy valued, long-term, trusting trade relationships typically share a significant interest in maintaining such a relationship because it offers assurances of enforceability. That is, the trading partners' business relationship is based both on economics and mutual reliance such that a dispute concerning a single transaction likely will be settled without invoking formal dispute resolution mechanisms. The value of the relationship—the confidence in its respective trading partners' integrity—outweighs the value of contesting a single transaction and potentially risking the unraveling of the trade relationship. Currently, when an error occurs that is not readily attributable to one of the trading partners, one partner may unilaterally agree to "take a hit" rather than accuse the other trading partner of error or fault and thereby risk harming their trading relationship. Thus, the clearinghouse enforceability mechanisms may not be as important to them as they would be to trading partners with less established trade relationships. Nevertheless, the clearinghouse could prove useful to trading partners who enjoy long-term trade relationships by reducing the possibility of errors, or, where an error occurs, quickly determining responsibility for the error, thereby reducing associated administrative costs and bolstering mutual goodwill. As electronic markets become more pervasive, strangers will frequently trade electronically; this will enhance the value of a clearinghouse.
5. **The value and associated risk of the transaction.**<sup>98</sup>

<sup>98</sup> For a discussion of risks in EDI transactions, see Baum, *Commercially Reasonable Security: A Key to EDI Enforceability*, Actionline, Nov. 1989, at 33-35. See Ch. 4.



6. **The required transactional speed.** For example, just-in-time manufacturing and transaction processing applications require expedited handling.<sup>99</sup>
7. **The cost of providing clearinghouse services.** Costs may remain variable or difficult to determine, but by extrapolating from the service costs of existing clearinghouse-like entities and value-added-network (VAN) services, a rough cost appraisal is possible.
8. **The availability of comparable services and the level of competition from clearinghouse-like entities and VAN services.**
9. **The requirements of specific applications, such as competitive bidding or transaction-proof capabilities.** Confidentiality, proof of timing of delivery, nonrepudiation, and confirmation of receipt, for example, will vary depending on the application.
10. **Other factors specific to trading partners' transactions and business relationships.**<sup>100</sup>

### § 5.14 Clearinghouse Enforceability Services

*Clearinghouse enforceability services* (CESs) are defined as those services that bolster the certainty and enforceability of electronic contracting. The following sections examine many possible services, including those that prevent message repudiation. Nonrepudiation mechanisms are designed to prevent a message sender from successfully denying the authenticity of the content of a message. This is of particular importance to contract enforceability. In addition, other major CESs relating to record holding, audit trail, and key-distribution and management are discussed.

<sup>99</sup> For example, under the Reynolds Co.'s Central Dispatch program, carriers are given one hour to accept or reject the load and another hour to arrange details for pick-up and delivery. Bonney, *Central Dispatch: \$4.5 Million Saved*, Am. Shipper, Dec. 1990, at 68. A Just In Time Delivery Message has been developed to permit "a customer to convey precise delivery sequence and Just In Time schedule requirements to a supplier. . . ." UN/EDIFACT Just In Time Delivery Message (DELJIT), vers. 0, rel. 4 (May 22, 1990).

<sup>100</sup> A contribution by the United States to the International Organization for Standards (ISO) proposes a conceptual model of EDI that includes a particularly broad category of services, many of which are relevant to the clearinghouse. These services include: methods of communication, translation/conversion services, naming & addressing, security, archival & retrieval, journaling & rollback, directories, marshalling & packaging, multiple content type and translation. Proposed Principles for Development of the Conceptual Model for Electronic Data Interchange, Doc. No. JT/89-0364-J, JTEDI/89 031, submitted to ISO/IEC/JTC1/SWG-EDI (1989).

### § 5.15 —Record Holding and Audit Trail

The EDI clearinghouse can serve as a document depository and trusted record keeper that holds a record copy of electronic transactions and related information intended to serve as probative evidence of the transactions. Record holding by a clearinghouse can simplify dispute resolution between trading partners when the content of each trading partner's records varies and yet each claims that its respective records are accurate and reliable.<sup>101</sup>

Consider the following example: Company A sends Company B a purchase order for five pollution scrubbers and Company B subsequently delivers 50 pollution scrubbers to Company A with an invoice requesting payment for 50. Company A asserts that it ordered only five pollution scrubbers; Company B claims that it received an order from Company A for 50 scrubbers.

In this example, the parties dispute the quantity of goods ordered. The parties could have agreed in a TPA or clearinghouse agreement that the copy of the transaction held by the clearinghouse would be considered the authentic record copy and would be binding upon the parties, provided that clearinghouse and trading partner rules pertaining to reliability and security were followed. Thus, in the event of a dispute involving transaction record integrity or authenticity, the parties would look to the clearinghouse record copy as the acknowledged official and accurate document.<sup>102</sup>

The parties must also decide precisely what data the clearinghouse must keep (for record copy purposes), in what form it is stored, how it is stored (storage medium), who may have access to it, and how long it is retained. Whether the parties require the clearinghouse to hold the complete official transaction record or, alternatively, a portion or summary of the original transaction record will depend in part upon:

1. **Privacy.** Some companies will not permit their data to be stored outside of their exclusive control. However, they may be more willing to permit a clearinghouse to store their data confidentially in encrypted or digest form (for example, a hash).
2. **Cost.** Clearinghouse data storage costs may permit only a subset of information to be held by the clearinghouse. This subset will generally comprise the most critical portion, such as purchase order control numbers, names of trading parties, product identification codes,

<sup>101</sup> See Ch. 4 on electronic records management.

<sup>102</sup> Accommodation must be made for instances when the clearinghouse is responsible for erroneous records. See Ch. 3 on TPSPA limitation of liability and correction of errors.

quantity and price information, or a hash or message authentication code (MAC) for the transaction.<sup>103</sup>

3. **Audit.** Trading partners may be concerned that, because of constraints in conducting audits beyond the boundaries of their respective entities, their auditors will not approve their reliance on clearinghouse-retained records. Auditing needs may require the maintenance of duplicate files by each company and by the clearinghouse.
4. **Technology.** The extent to which each of the trading partners implements technologies that provide assurances of privacy and authenticity will affect their need for clearinghouse enforceability services.

### § 5.16 Clearinghouse Structure

An EDI clearinghouse can be designed with varying degrees of centralization. The architecture of a clearinghouse will affect its functionality and the extent to which it may raise or diminish legal and control issues. This section discusses the functional considerations attendant to varying degrees of clearinghouse structural centralization.

A more centralized structure can provide:

1. Either more or less security. A centralized clearinghouse may provide greater security because controls are easier to administer and maintain in a centralized structure. Less security is provided by a centralized clearinghouse to the extent that users must relinquish more control over their confidential data.
2. More standard network management and control.
3. Consolidated and, consequently, more efficient administration.
4. Either higher or lower costs. Network structure and other considerations may result in higher communications costs, whereas data

<sup>103</sup> "A cryptographically computed value that is the result of passing text or numeric data through the authentication algorithm using a specific key. The message authentication code can be used as a hash or control total when text or numeric data must be protected from alteration." Security Structures transaction set, definitions.

A Message Authentication Code employs a unique code that is appended to the data stream. . . . [O]nly the appended code [need be] . . . encrypted . . . and the message remains in plaintext. This process, repeated by the recipient, must produce the identical code. If the codes are not the same, this is an indication that the code [or the data] being transmitted has been tampered with. The length of the appended code can vary, but the strength of the process is directly related to the length of the code.

National Computer Security Center, A Guide to Understanding Trusted Distribution in Trusted Systems, NCSC-TG-008 Version 1 § 4.4 (Dec. 15, 1988).

storage costs may be lower in a centralized system due to the reduction of redundancy and the creation of economies of scale.

A more distributed structure may provide:<sup>104</sup>

1. The benefits of newer applications, such as services utilizing client/server and remote access/query/call technologies to facilitate clearinghouse cooperative processing applications.<sup>105</sup>
2. Greater security. Services utilizing evolving distributed-system security standards and products provide greater efficiency and confidentiality to the user.
3. Increased flexibility. A distributed clearinghouse structure may best accommodate requirements for trading with many trading parties and diverse trading systems.
4. Reduced costs.
5. Either better or poorer technical performance which can affect accessibility, availability, and economy, depending upon the system's architecture, applications, and usage.

### § 5.17 Clearinghouse Connections

The manner in which TPSPs, trading partners, and other entities can and should connect with a clearinghouse can vary. Such connections can be direct or indirect. The extent to which a clearinghouse shares information with, and exercises control over, these connections and services varies, as may the nature of its record-holding services. Sections 5.18 through 5.21 describe the effect of different clearinghouse connection architectures on a clearinghouse's capacity to provide CESs.

### § 5.18 —Direct Intermediary Clearinghouse

The direct intermediary clearinghouse (see Figure 5-1) serves as the exclusive data communications channel—through which all transactions flow—

<sup>104</sup> A distributed system is made up of many building blocks or resources, such as individual workstation printing, filing, and mailing. One of the advantages of a distributed system is that resources can be reallocated according to need. Another benefit is that distributed resources can provide reliability through redundancy. Xerox, Clearinghouse, XSI 078404, at 5 (April 1984). More standards and better products for distributed computing will support a distributed clearinghouse.

<sup>105</sup> Client/server computing involves the physical separation of applications and data between or among programmable systems. Servers are increasingly negotiating tasks that previously were the exclusive domain of mainframes.



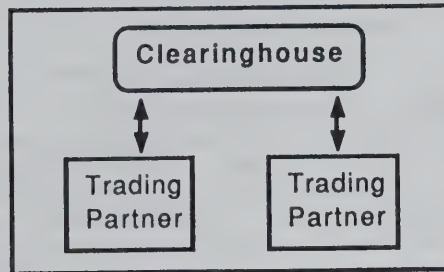


Figure 5-1. Direct intermediary clearinghouse.

between the trading partners. Contingent on agreement among all relevant parties, a clearinghouse can capture a copy of the transactions as they pass through. This architecture places a clearinghouse in the roles of both record keeper and TPSP.<sup>106</sup>

#### § 5.19 —Indirect, Record-Holder Clearinghouse

In contrast to the direct intermediary clearinghouse, the indirect record-holder clearinghouse (see Figure 5-2) does not serve as the primary communications channel for transactions. Rather, trading partners transact

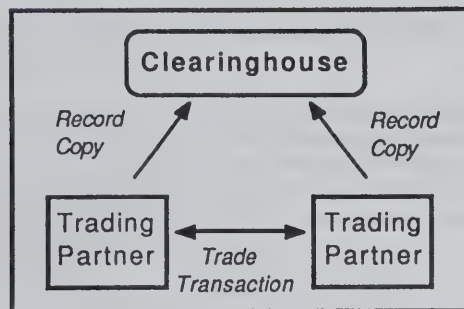


Figure 5-2. Indirect, record-holder clearinghouse.

<sup>106</sup> To the extent that a clearinghouse provides communications services. See § 5.2, which distinguishes attributes of TPSPs and clearinghouses.

directly and independently communicate a record copy of their transactions to the clearinghouse for record-keeping purposes. Each party must therefore trust that the record copy submitted to the clearinghouse is identical to the transaction communicated directly between the trading partners.<sup>107</sup>

Absent considerable controls, the indirect clearinghouse architecture structure is not particularly attractive because of the potential for a trading partner to send the clearinghouse a message that differs from that sent to the other trading partner. However, where a clearinghouse is used only to verify the match between trading partners' messages, or where message authentication codes and nonforgeable cryptographic techniques are employed, the indirect, record-holder architecture may prove of benefit.<sup>108</sup>

#### § 5.20 —TPSP Transfer Clearinghouse

A TPSP transfer clearinghouse (see Figure 5-3) serves as the depository of transactions communicated via TPSPs when the clearinghouse does not

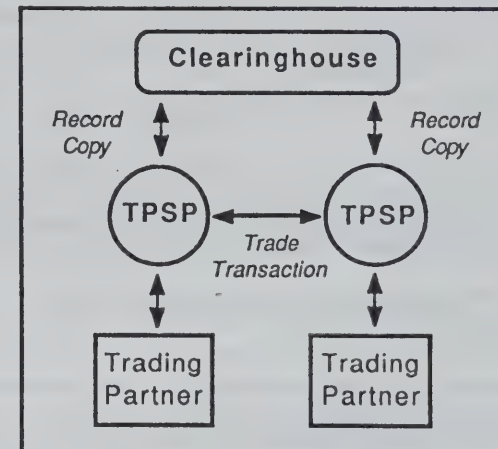


Figure 5-3. TPSP transfer clearinghouse.

<sup>107</sup> The extent to which trust is required will depend upon the data communications and computer environments. The use of cryptographic technologies may diminish the extent of trust required of each trading partner or of a clearinghouse in its record-keeping role.

<sup>108</sup> ASC X12 is developing, and X.400 recommendations already provide for a carbon copy (CC) feature, which may prove to be a useful tool for CES clearinghouse purposes. This

provide the communications channel for the underlying transactions. Transactions are originated by a trading partner, communicated through one or more TPSPs, and terminated with the other trading partner. The originating trading partner's TPSP submits a record copy of the transaction to a clearinghouse on behalf of that trading partner.

A TPSP transfer clearinghouse structure is conducive to TPSP accountability because a clearinghouse is apprised of, and records, TPSP transactions on behalf of the trading partners. Because the clearinghouse is sent an independent copy of all such transactions, the TPSP is discouraged from intentionally (or mistakenly) repudiating or delaying a transaction.

### § 5.21 —Second-Level TPSP Clearinghouse

An alternative architecture is the second-level TPSP clearinghouse (see Figure 5-4) in which all messages between the trading partners and between TPSPs pass through the clearinghouse via the primary communications

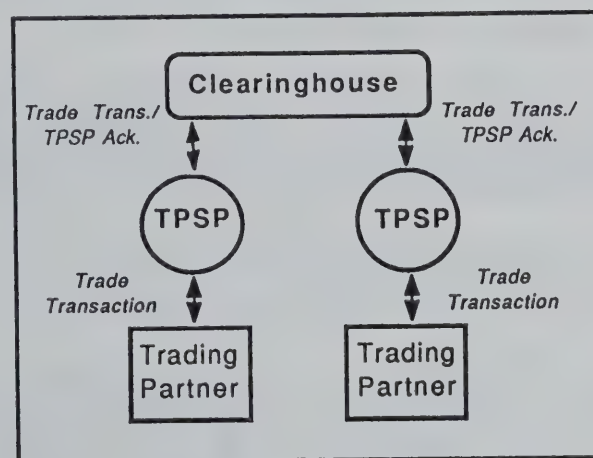


Figure 5-4. Second-level TPSP clearinghouse.

CC feature can randomly (when implemented with a randomizing program), periodically, or on demand create and communicate copies of trade messages sent to or through a clearinghouse, as well as send or hold them for predetermined auditors who are located within independent entities. See also the discussion of the UN/EDIFACT ENTRY message in Ch. 4.

channel. A clearinghouse would then capture and retain a record copy of these transactions (and TPSP acknowledgments).

This approach has the benefit of involving a clearinghouse in all transactions, but it may also involve additional communications costs. The Second-Level clearinghouse approach may put the clearinghouse in an advantageous position from which to provide notary-like services.

### § 5.22 P<sub>edi</sub> and the Clearinghouse

P<sub>edi</sub> and X.400 (1988) features, when properly implemented in conjunction with the EDI clearinghouse, can provide greater services and reliability. Figure 5-5 summarizes some of the services the combination of X.400/P<sub>edi</sub> and the clearinghouse can provide.<sup>109</sup>

Service	X.400	Clearinghouse	X.400/ Clearinghouse
Audit trail	•	o	+
Conformance testing	•(c)	o	+
Contract tracking		o	o
Developer of rules	•		•
Directory	•(a)	o	+
Information services	•	o	+
Key distribution	•	o	o
Nonrepudiation	•(a)	o	o
Notarial services		o	o
Performative services		o	+
Record holding	•	o	+
Trusted entity	•	o	+(b)

#### KEY

- —provided by X.400
- o —provided by the clearinghouse
- + —provided by X.400 with the clearinghouse
- (a)—provided in conjunction with X.500 directory services
- (b)—not provided by X.400, but as a trusted system X.400 supports this feature
- (c)—available through testing services

Figure 5-5. X.400/P<sub>edi</sub> and clearinghouse services.

<sup>109</sup>The clearinghouse is not intended to modify X.400 messages in transit. Therefore, when the clearinghouse is implemented in a P<sub>edi</sub> and X.400 environment, messages communicated through the clearinghouse would terminate at the clearinghouse (for



### § 5.23 Clearinghouse Functions Without Cryptography

Cryptography can enhance and supplement a clearinghouse's record-holding capabilities. Further, depending on the manner in which it is implemented, cryptography can satisfy certain security and reliability control objectives, such as various authentication, confidentiality, and integrity services. A clearinghouse that does not utilize cryptographic methods remains capable of providing some useful, but limited, clearinghouse enforceability services.

The following considers CES proof limitations when user-ID/password access controls, but no cryptographic methods, are implemented for authentication and integrity purposes.

**Identification of a user purporting to have originated a message.** A clearinghouse cannot prove with certainty who originated a message when an interloper purports to be a bona fide user. It can only prove that someone sent a message through the clearinghouse using a specific user-ID/password. It cannot authenticate the person who actually sent the message.

**Identification of the password ID of a user purporting to download a message.** A clearinghouse cannot prove who downloaded a message when an interloper purports to be a bona fide user. It can prove only that *someone* downloaded a message using a specific user-ID/password.

**Proving the time and date when a clearinghouse receives a communication.** The clearinghouse can date- and time-stamp messages<sup>110</sup> and maintain accurate logs of these events.

**Proving the time and date when the clearinghouse originates or forwards a message.** The clearinghouse can prove that a message was originated or forwarded from the clearinghouse, because such acts are under its direct control. However, the clearinghouse cannot authenticate the identity of the person who actually downloaded/received the message, only that *someone* using the recipient's user-ID/password downloaded/received it.

X.400 P<sub>edi</sub> purposes). The clearinghouse would initiate a new message, containing either the body of the received message and/or modified, value-added information, and forward it according to instructions. See Ch. 4 on X.400 and P<sub>edi</sub>. Note, reference to X.400 includes X.435. See Ch. 4.

<sup>110</sup> The time and date indication should be synchronized with the National Institute of Standards and Technology (NIST) standard atomic clock or should be implemented in some other coordinated manner. On time and date stamping legal issues, see Electronic Messaging, ABA Report No. 507-0210 (1988).

As a trusted record holder, the clearinghouse should, where commensurate with the risk and in conformity with legal requirements, provide stronger proof features than those provided by older acknowledgment and confirmation protocols, such as a conventional telex answerback.<sup>111</sup> Such a clearinghouse could provide better proof capabilities if it incorporated cryptographic methods. The benefits inuring to a clearinghouse from the use of cryptography are further explored within the context of key management.

### § 5.24 —Key Management and the Clearinghouse

Key management provides for the secure exchange of cryptographic keys for the purpose of facilitating secure communications. Chapter 4 briefly raised key-management issues. This section further describes key management and addresses possible key-management roles of the EDI clearinghouse.

Key-management standards for X12 EDI are modeled on the ANSI X9.17, a voluntary industry standard for financial institution key management (wholesale). Such standards are intended to provide:

1. Control of the keying material during the life cycle of the keying material to prevent unauthorized key disclosure, modification, or substitution
2. Distribution of keying material to permit interoperability between cryptographic equipment
3. Integrity of keying material during all phases of its life, including its generation, distribution, storage, entry, use, and destruction
4. Recovery of the key-management process in the event of failure or when the integrity of the keying material is questioned.<sup>112</sup>

In its most simple implementation, key management can be undertaken physically, such as by a courier or by registered mail. However, such physical key-delivery mechanisms have considerable shortcomings, and are not

<sup>111</sup> Telex features an *answerback* to identify the called telex machine. Upon connecting, the called telex sends a unique identifying message (an answerback) to the sending telex prior to and as a prerequisite of message transmittal. This does not provide a conclusively confirmed delivery, absent supplementary technology or procedures. The conventional telex's electromechanical pathways are riddled with possibilities for error. Errors and interruptions incident to telex service are "unavoidable" according to Western Union. Western Union Tel. Co., Tariff F.C.C. No. 240 § 4.6, Regulations (issued Apr. 4, 1983, effective July 3, 1983).

<sup>112</sup> Cryptographic Service Message Transaction Set, X12.42. See Proposed FIPS for Key Management Using ANSI X9.17.

further considered in this book.<sup>113</sup> This section addresses electronic key management within the context of key distribution and key translation, and § 5.25 considers public key certificate management issues.

A *key distribution center* distributes generated or acquired keys to parties that (1) wish to communicate with each other but may not currently share keys, (2) share a key-encrypting key pair with the key distribution center, and (3) may not have the ability to generate keys.<sup>114</sup>

A *key translation center* translates keys for future communication (1) between parties who wish to communicate with each other but may not currently share keys, (2) between parties who each share a key-encrypting pair with the key translation center, and (3) when the requesting party has (at a minimum) the ability to generate or otherwise acquire keys.<sup>115</sup>

Figure 5-6 depicts two potential trading partners who do not have a pre-existing contractual relationship and have not exchanged cryptographic keys. Each trading partner has, however, previously established a relationship with a clearinghouse in which the clearinghouse acts as a key center and independently shares unique secret keys (for example, a key-encrypting key) with each trading partner.<sup>116</sup>

When the prospective trading partners decide to engage in secure electronic trade, they can obtain and share a unique cryptographic key.<sup>117</sup> Using

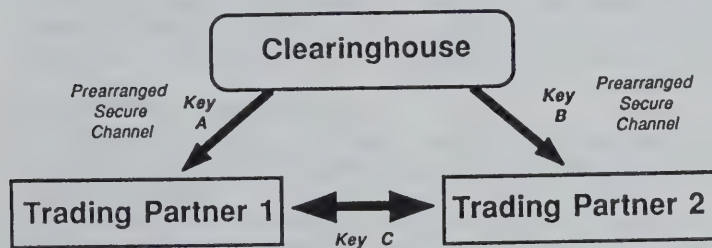


Figure 5-6. Simple clearinghouse key-management design.

a prearranged secret key (Key A) known only to the clearinghouse and to Trading Partner 1, Trading Partner 1 requests from the clearinghouse a unique secret key for trade with Trading Partner 2. The clearinghouse processes the request and, if valid, returns the unique secret key (Key C) to Trading Partner 1 using the prearranged secure channel between Trading Partner 1 and clearinghouse. Next, using a different unique, prearranged secret key (Key B), Trading Partner 2 independently receives from the clearinghouse a copy of Key C. Trading Partners 1 and 2 can then trade, using the new secure channel established between them with Key C, with assurance that the messages sent between them are securely communicated.<sup>118</sup>

This simple clearinghouse key-management design does not inherently provide either trading partner with assurances against transaction repudiation unless, for example:

1. The clearinghouse maintains a record copy of the transaction or a digest of the transaction, such as a MAC, or
2. Trading Partner 1 sends a copy of the encrypted (MACed) transaction to the clearinghouse using Key A (the key shared between Trading Partner 1 and the clearinghouse), and then the clearinghouse forwards the encrypted message (and a decrypted version) to Trading Partner 2, and the clearinghouse retains a copy of the transaction (encrypted using Key A). Such an encrypted message cannot be decrypted and authenticated by Trading Partner 2 without Key A, and thus Trading Partner 1 can neither decrypt nor modify the message without the cooperation of the clearinghouse. In a dispute between the trading partners, the encrypted message could be submitted to the clearinghouse by either Trading Partner for authentication and dispute resolution.
3. Or, the transaction is digitally signed within a properly implemented public-key (asymmetric) cryptosystem.

### § 5.25 —Public Key Certificate Management

Public key algorithms can support various clearinghouse services. In order to authenticate users and to provide assurances of the binding relationship between users and their respective public keys, potential trading partners who have not previously exchanged keys can use clearinghouse services to obtain needed assurances.<sup>119</sup> These assurances are provided by the clearinghouse or

<sup>113</sup> For example, couriers are much slower than electronic means of communication and a courier must be trusted. United States Postal Service registered mail does not require identification of sender and is subject to attempted modification by intermediaries. See National Computer Security Center, *Trusted Distribution in Trusted Systems*, NCSC-TG-008 Version 1 §§ 4.2, 4.3 (1988).

<sup>114</sup> X12.42 § 4.2.6.

<sup>115</sup> *Id.*

<sup>116</sup> Secret keys are described in the context of symmetric encryption in Ch. 4.

<sup>117</sup> This example involves symmetric key cryptographic methods only.

<sup>118</sup> The specific cryptographic methods and algorithms implemented will affect the extent to which parties have assurances that the communications are authentic, accurate, or confidential.

<sup>119</sup> Although public key cryptography may appear to provide for nonrepudiation without need for a clearinghouse or other trusted entity, a clearinghouse-like entity is needed for



other trusted entity when it issues a public key certificate, thereby certifying, among other information, that a specified public key belongs to a specified user. Such a certificate generally contains the trading partner's name, the certificate issuer's name, validity-period information for the certificate, the trading partner's public key, key algorithm identifiers, and the issuer's digital signature.

A clearinghouse that issues certificates is said to be serving as a *certification authority* (CA). In its capacity as a repository for certificates issued by CAs, a clearinghouse functions as a *certificate repository*. For transaction authentication and integrity verification purposes, the transaction originator's certificate is evaluated by the transaction recipient to validate the binding between the originator and its CA.<sup>120</sup> Validation can involve extracting the CA's public key and using that value to decrypt the transaction's digital signature.<sup>121</sup> For confidentiality purposes, when the recipient of an encrypted transaction desires to decrypt and read it, the recipient validates the originator's certificate and then uses the recipient's private key to decrypt the message (or to decrypt another key, such as a DES key, when such a key was used to encrypt the body of the transaction for privacy).

### The Certification Authority

The CA is an entity that is trusted by the trading partners to create and assign certificates. The CA's responsibilities should include verifying that the information contained in certificates it issues is accurate. The extent to which a CA vouches for the information contained in a certificate affects the reliability of underlying electronic transaction records; the reliability of public key cryptographic methods consequently requires trustworthy CAs. In order to instill confidence in its CA capability, the clearinghouse should make available details of the technical and procedural safeguards it employs, including independent audit reports.<sup>122</sup>

certificate management purposes. The main exception is when parties have previously exchanged public keys directly (*out-of-band*, such as by courier) and have assurances of identity and authenticity of the binding between their trading partners and their respective public keys and have provided for notification in the event of key compromise. However, out-of-band practice is inconsistent with ubiquitous communications and is therefore not treated as an appropriate model for open trading practices.

<sup>120</sup> The extent and expectation of the required binding, or relationship between the CA and the originator, can vary according to the implementation.

<sup>121</sup> Certificate validation involves verifying that the certificate issuer's digital signature affixed to the certificate is valid, that is, the one-way hash value computed on the certificate's contents matches the value that results from decrypting the CA's digital signature using the public key of the CA.

<sup>122</sup> Except to the extent that such disclosure might compromise clearinghouse security.

When multiple trading partners hold certificates issued from other CAs, each CA requires mechanisms to validate certificates issued by the others. The authenticity of certificates issued by entities within the same certification hierarchy can be ensured by the chaining of certificates from the originator's CA all the way to the root of the certification hierarchy.<sup>123</sup> Thus, when there are multiple levels of CAs, a superior CA should certify a subordinate CA. The chain of certifications would be evaluated until the top of the certification chain is reached.

Validation of certificates issued by CAs from different certification hierarchies also can be facilitated by cross-certification. When two trading partners hold such certificates, *cross-certification* conventions are used to validate them. Cross-certification may occur within the context of a root (top-level) CA issuing a certificate to another root CA (that is, in which the other is the subject of the certificate) and in the subsequent validation of such certificates. See Figure 5-7 below.

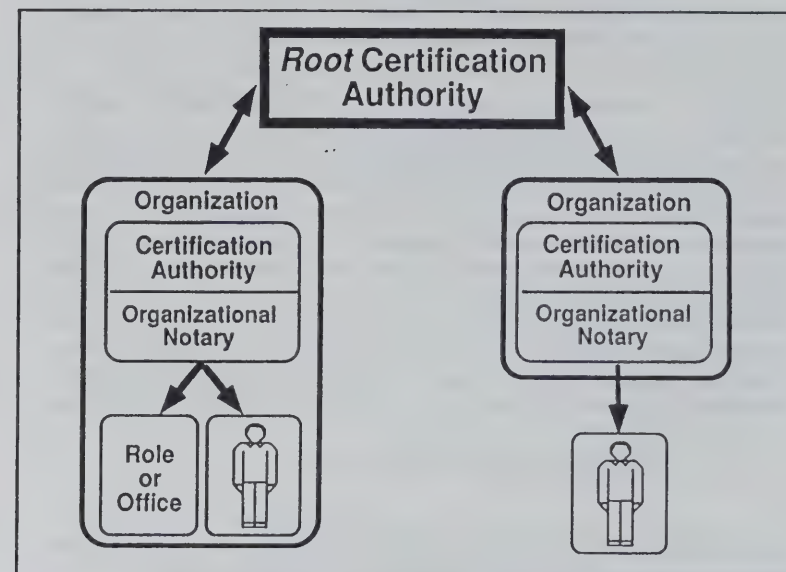


Figure 5-7. Certification authority.

<sup>123</sup> A certification hierarchy can take the form of a tree in which each node is a CA and each arc represents a certificate in which the superior node is the issuer and the inferior node is the subject of that certificate. See also Ch. 4 concerning chaining of notarial certificates of acknowledgment.

Figure 5-7 represents only one certification hierarchy architecture, although it may nonetheless prove the most rational. Note that under X.509, one can cross-certify both subjects and CAs. One purpose would be for a variety of root certification authorities to cross-certify themselves.

Trust is critical in cross-certification, as well as in certification issuance and revocation:

An entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function. The key role of trust in the authentication framework is to describe the relationship between an authenticating entity and the certification authority; an authenticating entity must be certain that it can trust the certification authority; and the authenticating entity must be certain that it can trust the certification authority to create only valid and reliable certificates.<sup>124</sup>

The law neglects to specify the expectations of trust in cross-certification or the obligations of integrity implicit in certificates that originate in other certification hierarchies.

It is essential that users have assurances of the integrity of the top-level CA in the hierarchy. Who should be the highest CA in the chain? What are the essential attributes of the root CA? Clearly, it must be an impeccably trustworthy entity. Some security experts argue that it should be a Regional Bell Operating Company, AT&T, a central bank such as the Federal Reserve, or some other large entity that enjoys the public's trust.<sup>125</sup> The financial ability of the root CA to indemnify injured users (to the extent of its legal obligations) should also be a consideration; arguably, this would militate toward placing the Federal Reserve Bank or a recognized government institution in this role.<sup>126</sup> With respect to international transactions, an international organization such as the United Nations might be an

<sup>124</sup>International Telephone & Telegraph Consultative Comm., CCITT X.509 § 3.3.n, Doc. No. AP IX-47-E (Apr. 1988).

<sup>125</sup>However, regulatory considerations may restrict the range of possibilities. See § 5.43 concerning telecommunications regulatory issues.

<sup>126</sup>For government-related transactions, the General Services Administration is considered a root CA candidate because of its historical role in providing key management. The United States Postal Service is also considering a key-management role because it (1) is highly distributed; (2) has considerable experience in administering certified and registered mail, as well as providing notifications and certificates of delivery; and (3) is concerned about remaining competitive with electronic communications services (for example, the Postal Service previously but unsuccessfully entered the electronic mail market with its ECOM product), which have been eroding the service's market share, and (4) offers an existing national automated directory capability through its ZIP code data base.

appropriate root CA.<sup>127</sup> Can or should we ultimately trust anyone? If we do not, a key-management system will not serve its intended purpose. The top-level-certification authority issue has been sardonically expressed as a question of "Who is God?"

### Certificate (or Security Credential) Repository

Generally, a clearinghouse can store certificates and make them accessible to the trading public as a certificate (or security credential) repository whether or not it also serves as a CA. However, when a clearinghouse serves only as a certificate repository, it acts as a security-credentials database. International standards have been developed to provide for an electronic directory (the Directory) that, among other functions, can hold trading partners' security credentials. Figure 5-8 describes the security credential depository within the context of the CCITT X.500 directory recommendations. The Directory is further described in § 5.28. The security credential repository can operate in this manner: The Directory holds the security credentials (which can include certificates) of trading partners. For authentication purposes, a trading partner can query the Directory to obtain the

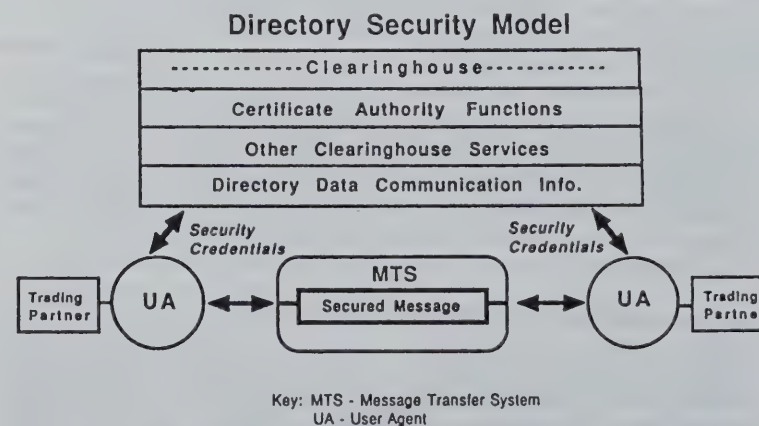


Figure 5-8. Clearinghouse security credential depository.

<sup>127</sup>For example, the United Nations International Telecommunications Union (ITU). However, not all persons, corporations, and governments trust the United Nations, or for that matter any other particular international institution.



security credentials (for example, the public key certificate) of a trading partner. For public key purposes, the evaluation of the certificate (checking the validity of the digital signature and the content of the certificate) provides assurances of the authenticity and integrity of a corresponding digitally signed transaction. The originating trading partner could then initiate a secured transaction through the message transfer system (MTS).<sup>128</sup> For privacy purposes, the originating trading partner desiring to engage in confidential communications with another trading partner would query the Directory for the intended recipient's certificate (to obtain and confirm the validity of the recipient's public key). The originating trading partner would then encrypt the communication for privacy, using the recipient's public key. This would provide privacy, because only the recipient could decipher the message. Upon receipt and validation of the intended recipient's security credentials from the Directory, the originating trading partner would then initiate with assurances of authenticity or privacy a secured message through the MTS.

### § 5.26 Clearinghouse Expediting Services

Services that could help trading partners more readily learn about each other, their respective products/services, and their business and contracting procedures are addressed next. Clearinghouse or affiliated clearinghouse-supported database services constitute the centerpoint of clearinghouse expediting services. Many of these services also have the effect of further ensuring electronic transaction record reliability.

### § 5.27 —Database and Information Services

A clearinghouse can provide important and innovative information services to the electronic trading community. These services fall into two main categories, trading partner information and general trading information.

#### Trading Partner Information

Trading partner information includes company-specific financial data, logistical/shipping data, authorization(s) for electronic trading, government representations and certifications,<sup>129</sup> sales terms and conditions, banking and other financial data, supplier ratings, alerts, awards, surveys, and

product information. The dissemination of such information can further be facilitated by:

**The customer profile transaction set (CPTS).** The CPTS is an X12 transaction set that is intended to facilitate the general exchange of trading partner profile data between trading partners.<sup>130</sup> It could be used to communicate trading partner profile information to the clearinghouse in order to (1) expedite the contracting process, (2) prevent the need to rekey profile-type data upon its receipt by a trading partner, (3) improve data accuracy, (4) automate data transfer, (5) enhance control/security and data accessibility, and (6) expedite profile updating.

**Proposed trading partner agreement terms and conditions transaction sets.** Trading partners could evaluate their counterparts' contract terms and conditions prior to trading, without awkward or untimely personal requests for information.<sup>131</sup> The database could also tag a unique number-identifier to each paragraph or clause of the trading partner agreement, as well as to boilerplate terms and conditions. Trading partners then could easily reference, and/or incorporate by reference, the applicable tagged clauses in their transactions.

**Authorization to be bound to published agreements.** Trading partners could agree to industry/trade association or other published terms and

<sup>130</sup> See ASC X12 Project Proposal, *Transaction set(s) for the exchange of trading partner profile data*, Doc. No. ANSI/X12B/PP-067 (May 18, 1988). See also Memo from Michael Gerus, project team coordinator, to Automobile Industry Action Group (AIAG) Departments (Dec. 19, 1989). Subject to reasonable restrictions, the CPTs could also communicate other data of commercial trade value, such as the underlying terms and conditions of anticipated sales transactions and specific government reporting data.

<sup>131</sup> [EDI is] typically touted as a mechanism to significantly reduce the amount of paper flow in business transactions. However, current EDI standards do not yet provide for the automated and machine processable communication of underlying terms and conditions of business transactions (including trading partner terms and conditions). This proposed transaction set intends to provide an EDI mechanism for the communication and processing of such terms and conditions, and possibly to include payment terms. . . .

In the absence of the proposed transaction set, contractual data must generally be communicated "out-of-band", that is outside of EDI. This practice will increasingly become inconsistent with commercial needs. It should be noted that the ASC X12 Text Transaction Set (and the EDIFACT General Message (GENERAL)) provide for the communication of "free text", but is easily abused and its use is discouraged. Moreover, the Text Transaction Set does not provide for the communication of structured information, while the proposed Contract Transaction Set would provide for both structured and unstructured information.

Baum & Savage, *Proposal for the Contract Transaction Set* (a white paper prepared for X12's Legal and Business Controls Task Group), ASC X12X/TG1/90-156 (1990).

<sup>128</sup> See Ch. 4 concerning the MTS.

<sup>129</sup> See Federal Acquisition Rules (FAR) 48 C.F.R. § 52.301 (1990). See Ch. 7.

conditions, code(s) of conduct, or guidelines. The clearinghouse could also offer an on-line clause/code list by which trading partners could automatically create full-text versions from the encoded data.

### General Trading Information

General trading information can include industry financial statistics, industry and multimodal transportation logistics data, supply and demand data, and inflation indexes. The information provided by clearinghouse databases need not originate from the clearinghouse or from clearinghouse users, but could come from independent interconnected service providers.<sup>132</sup>

### Clearinghouse-Derived Information

Information compiled or derived by the clearinghouse, such as cumulative statistics on clearinghouse-based transactions, network use, transaction volumes, audit reports, and billing and status data, could provide useful strategic information to clearinghouse users<sup>133</sup> and could help to expedite transactions.

## § 5.28 Directory Services and the Clearinghouse

A global, highly distributed, hierarchical directory service<sup>134</sup> could provide access to trading partner communications addresses, communications capabilities, security credentials,<sup>135</sup> and possibly trade terms and information.<sup>136</sup> A clearinghouse could then provide or participate in directory services either directly or through other directory entities and resources. Figure 5-9 illustrates the simple provision of directory services. In both cases, potential trading partners could query the directory for a wide range of information, or, at a minimum, reference the directory for supplemental information sources to expedite trading.<sup>137</sup>

<sup>132</sup> For example, the Universal Product Code (UPC) database provided by GE Information Services and the Duns Number and United States government Standard Industrial Classification (SIC) code database provided by Dun & Bradstreet.

<sup>133</sup> Great caution must be exercised in the provision of clearinghouse-derived information because of privacy and antitrust considerations.

<sup>134</sup> See CCITT X.500-509, electronic directory services recommendations.

<sup>135</sup> See § 5.25.

<sup>136</sup> Directory services and the referenced directory recommendations are capable of being implemented independently of a clearinghouse. This discussion merely proposes that a clearinghouse and directory can mutually benefit from their joint implementation.

<sup>137</sup> See § 5.29.

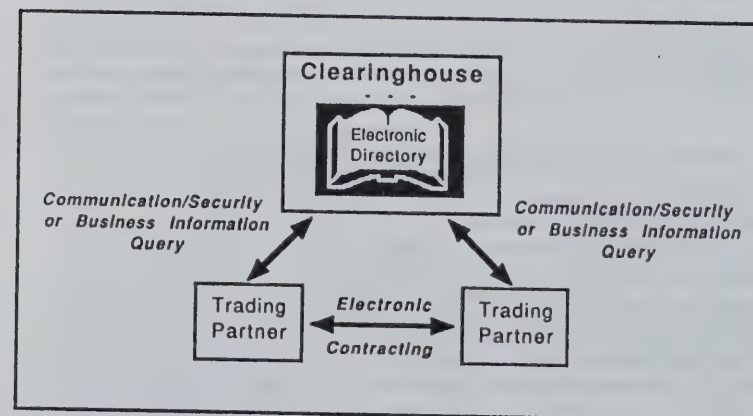


Figure 5-9. Clearinghouse directory services.

No clearinghouse can support all potential directory references; rather, a clearinghouse requires directory support from other entities. Access to comprehensive directory resources may raise legal issues such as data privacy and accuracy and the timeliness of directory updates.<sup>138</sup> According to one expert, the "biggest problem to be addressed . . . is that of information sharing. 'We don't want to share proprietary information . . . but we can share distinguished information (such as an individual's name and location).'"<sup>139</sup> The chairman of the North American Directory Forum, a consortium of North American electronic messaging services, has noted that "[p]articipants have already indicated a willingness to share knowledge. . . . This is a key condition for building a truly distributed directory, and we have laid out the preliminary requirements for sharing information."<sup>140</sup>

The possible functions of an electronic white pages service in a communications network must be flexible.

Because local information is made available through the white pages service, this argues for both distribution of information (each local organization will wish to maintain their own "part" of the white pages), and access control (some information, such as internal telephone numbers, may be "company confidential"). Every organization has some directory information that should not be openly published.

<sup>138</sup> See M. Rose, *The Open Book* (1990) for a detailed discussion of directory issues and architectures.

<sup>139</sup> Ron Wheeler, *interview published in EMA Update 2* (Electronic Mail Ass'n Fall 1990).

<sup>140</sup> Donald P. Casey, *quoted in EMA Update 2* (Electronic Mail Ass'n 1990).



In addition to containing infrastructural information for the network community, the white pages service may also contain network information for listed users of the network. Of these, the most notable is a user's electronic mail address. Of course, other information, such as passwords and access rights, might also be available from the white pages service.

Finally, the programs which run in the network make use of the white pages service for other purposes. For example, a sophisticated network management program might use the white pages service to obtain information about the computers attached to a particular physical network (e.g., contact information for the system administrators of those systems) in order to perform some task (e.g., notify those administrators of problems).<sup>141</sup>

Determining the best directory services model for EDI clearinghouse implementation is not a trivial matter. Database technological and structural considerations, business needs, and other factors must be considered. Some industry experts assert that the X.500 directory model is implementable in a multinetworked, multicompany environment, while others suggest that only one or a few major communications providers, such as AT&T, can successfully implement the directory because of its complexity and magnitude. Moreover, because AT&T already provides a successful telephone directory, it is in a stronger position to undertake global electronic directory services than other communications providers.<sup>142</sup>

### § 5.29 —Business Information Attribute

A directory attribute has been proposed to provide business contractual information through directory mechanisms.<sup>143</sup> The information would be

<sup>141</sup> Rose & Schoffstall, *An Introduction to a NYSENet White Pages Pilot Project*, NYSENet, Inc., Jan. 12, 1990, at 3.

<sup>142</sup> Multiple vendors will likely provide X.500 compliant directories in 1991. AT&T recently announced that it will provide computer access to its directory for some of its corporate customers. *Comms. Week*, Jan. 15, 1990 at 32. Pacific Bell has not contracted for this service because of privacy concerns.

<sup>143</sup> Baum, *Proposal for a Business Information Attribute X.500*, submitted to the NIST Directory Special Internet Group (June 1989) and the Special Internet Group's corresponding liaison report to the ASC X3T5.4 (a work group concerned with the X.500 Directory recommendations), *Directory Services Support for Business Information* (June 19, 1990). Subsequently, JTC1/SWG-EDI suggested that SC18 request establishment of a new work item to develop a standardized means for information object references, which is ostensibly consistent with the above ASC X3T5.4 proposal.

The JTC1 proposal states that:

[R]etrieved entries (from the object class Application Process or Application Entity) would be references to specific information objects the client desires to access. Additional information contained in the Directory entries would enable the client to contact the information reference directly for specific business

provided by the clearinghouse. The business information attribute would provide a pointer to various business information, such as trading terms and conditions and price lists, or to information within the directory itself. Although the X.500 directory is not intended as a general-purpose information database, trade data that facilitate business communications ultimately should be considered within the directory's scope.<sup>144</sup>

### § 5.30 —Naming

A clearinghouse can serve as a naming authority to administer the registration of data communication user identification information—trading partner names and associated attributes, including security credentials.<sup>145</sup> The clearinghouse could implement a naming approval procedure to ensure that (1) trading parties are uniquely identified, (2) directory entries are accurate, and (3) confusion among named entities is minimized. Naming authorities' practices and their coordination will become increasingly important in ensuring the reliability of electronic transactions.<sup>146</sup>

### § 5.31 Conformance and Other Testing

Testing electronic trading software, hardware, and systems can contribute to the reliability of electronic transactions and thereby enhance the legal enforceability of electronic trade transactions. Various testing methods have concomitant benefits and shortcomings. This section identifies the relative merits of two major classes of testing: *conformance* and *interoperability*. It also considers proprietary, industry, and interindustry testing

information. Clearly, there are two options available for looking up entries in the Directory. . . . In either case the client would have sufficient information from the Directory entry to contact the specific information object (service) directly.

<sup>144</sup> Because the directory model permits organizations to specify object classes and attribute types.

<sup>145</sup> Preferably, only when user names are immediately subordinate to the clearinghouse.

<sup>146</sup> An Organizational Relationships transaction set (816) is under development "to transmit pertinent information about a parent organization, its members and the relationship of a member to the parent organization; identify eligibility to purchase under the terms and conditions negotiated by a parent organization on behalf of its members; and to update application databases." However, it is not intended to convey personal information.

The American National Standards Institute (ANSI) has established a registration authority for the United States to register organization names consistent with the authority vested in ANSI as the U.S. member body of the International Organization for Standards (ISO) DIS 9834-1, *Information Processing Systems-Open Systems Interconnection-Procedures for the Operation of OSI Registration Authorities*. See ANSI Doc. USA RAC 024 (April 1991).

regimes in practice. The section concludes with a description of possible testing roles of the proposed EDI clearinghouse.

Conformance testing assesses and verifies implementation performance in accordance with a particular specification or standard, such as OSI,<sup>147</sup> ANSI X12, or GOSIP.<sup>148</sup> While such testing raises confidence in the likelihood that applications will interoperate, it does not ensure interoperability. Conformance testing can identify data that potentially may be misprocessed to help prevent trading partners from misinterpreting data and then mistakenly accepting or discarding it. Arguably, if deviation from the standards conformance is allowed, the standards and conformance testing regime will become less useful.

Implementing the X12 or UN/EDIFACT syntax correctly is a rigorous process. Conformance testing can be used to identify and resolve differences in syntax usage. Within the X12 environment, testing has focused largely on conformance to the structures and syntax of the Application Control Structure of X12.6.<sup>149</sup> This testing evaluates conformance to the basic X12 structure; the proper use of syntax, character sets, delimiters, data elements, data segments, transaction sets, functional groups, and control segments (such as loops and nesting); and proper relationships among the various building blocks of X12 transactions.

Some TPSPs undertake to test all transaction sets in order to protect the intended recipient from receiving a transaction set it cannot process. Other testing is available for messaging system communications protocols.<sup>150</sup>

Many companies require some form of testing as a prerequisite to sending legally binding "live" EDI or EFT transactions, to ensure that the transmitted data is received and processed into the partner's computer and its data fields are interpreted as intended.<sup>151</sup> The type and method of testing

<sup>147</sup> See Ch. 2 on OSI.

<sup>148</sup> See generally Government Open Systems Interconnect Profile (GOSIP) Conformance and Interoperation Testing and Registration, Version 1.0 (NIST Sept. 1, 1989) [hereinafter GOSIP Conformance]; OSI Conformance Testing Methodology and Framework Part 1: General Concepts, ISO DIS 9646-1 (ISO May 1988).

<sup>149</sup> See Ch. 2 for a description of X12.6 structures.

<sup>150</sup> For instance, The Corporation for Open Systems International (COS) offers message handling system testing. COS, Customer Guide to COS Test Services, Doc. No. COS/OPS-89/005 5/18/90, at 6 [hereinafter COS].

CCITT 1984 X.400—Message Handling Service. The COS MHS Test system is designed to aid in the evaluation of conformance to the CCITT X.400 series P2 protocol, P1 protocol, Reliable Transfer Service ("RTS") protocol, and the X.225 Session protocol. The COS MHS test suite covers the X.400 series P2, P1, and RTS protocols and have been taken from the draft CCITT testing specifications and have been aligned to the December 1987 NBS Implementor's Agreements.

COS at 6.

<sup>151</sup> See Ch. 2 on testing requirements in trading partner agreements. Becoming an EDI Partner with Alcoa, EDI Partner Information Packet § IX (June 24, 1988).

varies. For example, the Aluminum Company of America (ALCOA) requires each of its trading partners to determine:

with the Alcoa EDI Coordinator, the type of "test" that will be conducted. Method (a) listed below is the recommended and preferred.

- a. "Turnaround" of the Alcoa test purchase order. *[This is a software test in which purchase order data is communicated and communicated back ("flipped") between Alcoa and its trading partner.]*
- b. Trading Partner will create a "test" invoice from scratch.
- c. Trading Partner will send "live" invoice data on an active EDI purchase order. This method is least preferred as duplicate hard copy invoices can result in double payment. . . .

Once the test invoice has been sent, it will be evaluated by Procurement and Invoice Approval personnel to ensure correct routing and content.

Upon successful testing, the Alcoa EDI Coordinator will advise the date to begin sending invoices in production as well as when to eliminate the mailing of hard copy invoices.<sup>152</sup>

Transactions involving the mailing of hard copy are duplicative and costly, particularly where each hard copy transaction is reconciled with an electronic transaction. Nonetheless, many experienced EDI managers assert that they would never accept an EDI transaction without a trial period during which paper and electronic transactions are communicated in tandem.

## § 5.32 —Interoperability Testing

Whereas conventional conformance testing focuses on achieving conformity to technical standards, interoperability testing is designed to ensure actual reliable electronic trading. Interoperability testing duplicates the real-life environment in which an implementation will be used,<sup>153</sup> and is primarily oriented to serving practical user needs. Interoperability testing is performed between, for example, two communications/computer platforms to assess the ability of trading partners' EDI systems to effectively communicate and the capability of the respective application systems to accept the EDI information. For instance, an order entry system must be capable of accepting information received in a purchase order transaction set.<sup>154</sup> Timing issues, such as those related to the sequence of transaction delivery,

<sup>152</sup> Becoming an EDI Partner with Alcoa, § XIII, Invoice (810) Transaction Implementation Procedures, ¶¶ 5, 7 (Dec. 1, 1990).

<sup>153</sup> FIPS PUB 146 at 11.

<sup>154</sup> The X12 purchase order transaction set's PO1 segment provides for ordering a line item. It allows the product to be identified in a number of ways, for example, by buyer's part



inherent system or processing delays, and system availability, can be critical to interoperability testing and must be considered.<sup>155</sup> A platform may have passed conformance tests to a given standard, yet could still fail in its ability to interoperate with other platforms.

Potential limitations to various forms of testing include the following:

1. As trading partners develop more intimate and sophisticated relationships, their respective implementations acquire uniqueness and greater specificity, which renders them less amenable to and less able to benefit from standardized testing.
2. Testing may favor a buyer over a seller because disparities in their relative bargaining power may require the seller to change its system to accommodate or benefit that of the buyer.
3. Interfacing a company's systems and data with those of another company can be difficult. While *syntax* testing has many limitations, it is implementable and somewhat straightforward; *usage* testing of the standardized formats is more useful but more difficult.
4. Hidden issues such as changes in either party's internal systems, as well as the life cycle of any standard, may affect testing.
5. More recently, interoperation testing has been identified as a necessary step in demonstrating interworking of Open Systems implementations. Whereas the failures in conformance testing likely will be software errors, interoperation problems appear more likely to include problems of parameter range selection, attempts to use incompatible protocol stacks, attempts to use optional functions not implemented, and failures to implement mandatory functions.

Testing by third-party entities, such as industry associations, independent laboratories, or the clearinghouse, presents new challenges and choices. For example, the Automobile Industry Action Group (AIAG) coordinated a Minimum Micro-Computing Turnkey Package Approval Procedure<sup>156</sup> conformance testing regime:

Following the commitment by the North American Auto Manufacturers to computerize communications with their supplier community, the AIAG recognized the need of the smaller supplier for help in adapting to this new technology. The AIAG has encouraged the development of hardware/

number, vendor's catalog number, UPC number, or federal stock number. The extent to which such information is used and represented in transaction sets varies and is not sufficiently resolved by standards. Interoperability testing can identify these problems.

<sup>155</sup> The time at which responsive transaction sets are communicated will depend on the trade relationship and the type of operation.

<sup>156</sup> See Memo from Irv Chmielewski, assoc. dir. of the AIAG, to software developers (Nov. 1988) [hereinafter AIAG].

software packages at the *microcomputer* level. The objective is to assist those suppliers that lack expertise in the development or selection of an appropriate system or package.

To insure the microcomputer packages meet certain minimum requirements of the auto industry, the AIAG is coordinating a program whereby such packages are approved by the Auto Manufacturers themselves. A developer who chooses to seek such approval enters into a two-phase process through the AIAG. Each of the Manufacturers (Ford, Chrysler, AMC and GM) notifies the AIAG when a particular package has been approved. The AIAG then publishes, upon request the up-to-date status of developers involved in the approval program.<sup>157</sup>

\* \* \*

The AIAG Test regime consists of two phases. Phase I includes: "[a] Demonstration of Electronic Data Interchange with Individual Automotive Manufacturers," and a requirement that "[e]ach automotive manufacturer will provide a test material release file which the System Developer will retrieve electronically and from which the System Developer will create and transmit a test Advance Shipping Notice ("ASN")." Phase II includes: "[a] Demonstration of Turnkey System Operation."<sup>158</sup>

The AIAG testing was explicitly intended for a specific purpose and is limited to only two transaction sets. It is also an intensive mass certification program aimed at bringing up trading partners within a short time period.<sup>159</sup> However, it does go beyond simple syntax testing.

Sponsored by the Office of the Secretary of Defense, the Computer-aided Acquisition and Logistics Support (CALS) Test Network (CTN) is another testing program relevant to EDI. The CTN's objectives include the development of distributed testing capabilities to evaluate the effectiveness of CALS standards, which define the interchange of digital technical data.<sup>160</sup> The CTN includes conformance and user application tests<sup>161</sup> and is intended to:

[a]fford an opportunity to evaluate standards in the context of existing systems. Testing can be expected to identify system incompatibilities and

<sup>157</sup> AIAG at 3.

<sup>158</sup> AIAG at 2. The AIAG further states that

[A]t the system demonstration, the system developer must: Be prepared to transmit and receive "ASN" and material release records from each manufacturer that has approved the system developer's electronic data interchange . . . [and be] prepared to demonstrate variable data element formats relative to TDCC or ANSI table driven specifications.

<sup>159</sup> However, as a limited test regime, implementation still requires considerable trading partner expertise.

<sup>160</sup> CTN Handbook 9 (Dep't of Defense Dec. 1989).

<sup>161</sup> Military Specification MIL-M-28001. For example, it also includes testing to Standard Generalized Markup Language (SGML) standards. See § 5.38 on SGML.

weaknesses that must be corrected to employ CALS standards. Testing in the context of the CTN will assist in the resolution of industry/government wide problems. Some testing will fulfill specific program requirements to demonstrate a CALS compatible capability. It is important that testing be adequately documented to provide the maximum benefit to all involved parties and to avoid inadvertent duplication. All . . . participants need to be informed of testing conducted inside and outside the . . . [c]ompany to allow an incremental approach to integrated testing.<sup>162</sup>

The Government Open System Interconnection Profiles (GOSIP), which are compulsory and binding for all government solicitations and contracts for the acquisition of network products, also include conformance testing and some interoperability testing requirements.

### § 5.33 —Testing Certifications

Upon successful completion of testing,<sup>163</sup> the product or system tested is typically certified by the testing entity. The effect, value, and liabilities associated with certification are important to consider. For example, one testing consortium, the Corporation for Open Systems International (COS)<sup>164</sup> offers the COS Mark as an independent indication that tested products meet COS requirements.

Products awarded the COS Mark:

- Have passed a specific set of COS tests, indicating conformance to a COS Stack Specification.
- Represent an increased likelihood of interoperating with other COS Marked products conforming to the same stack.
- Are sold by a vendor that has obligated itself to attempt to resolve interoperability problems between COS Marked products of different vendors should they arise.

<sup>162</sup> Shoop & Doyle, Boeing CALS Project Test Plan 12 (Aug. 1989).

<sup>163</sup> As this material on conformance and other testing suggests, testing can take many forms. Unless otherwise specified, testing in this discussion is considered generically. Testing could, for example, be performed for syntax, applications, and boundaries between protocols.

<sup>164</sup> Customer Guide to COS Test Services, COS/OPS-89/005 (May 18, 1990) [hereinafter COS Guide] (COS), at 4. COS is "a consortium of information technology vendors and users. COS's mission is to provide an international vehicle for accelerating the introduction of interoperable, multivendor products and services operating under agreed to OSI, ISDN, and related international standards." *Id.* Examination of COS in this book is in the context of an organization that does testing; it is not necessarily intended to suggest that the testing COS undertakes is either sufficient or appropriate for EDI.

- Are supported by COS's agreement to make available certain resources to render a technical opinion if vendors and customers cannot agree on the cause of a failure of COS Marked products to interoperate.<sup>165</sup>

Also in the area of testing certification, successful completion of AIAG coordinated testing results in a designation of approval: "When Phase II approval is granted by the Manufacturer's Review Team, the System Developer will be free to mention in any sales or promotional material that the system has been approved by AMC, Chrysler, Ford, and GM through the AIAG."<sup>166</sup>

### § 5.34 —Testing Responsibilities

The responsibilities and liabilities of testing entities are issues of importance because organizations will not agree to offer testing without assurance of limited risk and because the responsibility undertaken by the testing entity can affect testing certification.

### § 5.35 —Transaction Flow Testing

In addition to certifying the simple syntactical conformance or the basic interoperability of discrete transaction sets, testing could extend to use of an architectural model and evaluation of the series of discrete transactions that are intended to result in a binding electronic contract. Sophisticated testing could evaluate the interrelationship and logical flow of transactions among the entities with the intention of determining not only that basic technical requirements are met, but also that the transaction flows are consistent with perceived administrative and legal needs. For example, the series of purchasing and payment transaction sets in Figure 5-10 illustrate the testing of a series of transactions relating to a specific purchasing activity.

Given the scope of variables and complexities involved, testing transaction sets is indeed a very difficult task. Difficulty is a compelling argument for the development of a default set of EDI transaction sets or UN/EDIFACT messages that facilitate accurate and meaningful testing between potential trading partners and are available on a *voluntary* basis.<sup>167</sup> This

<sup>165</sup> COS Guide, at 5.

<sup>166</sup> AIAG, at 2. A software product can only be tested to be in conformance with a given standard. Application-level testing can be performed only for conformance to a specific set of internal industry or organization standards that primarily involve the use of the data transmitted.

<sup>167</sup> See Norris, *Corporate Strategies and Tools for Making EDI Standards Work*, EDI F., 1990, at 102.



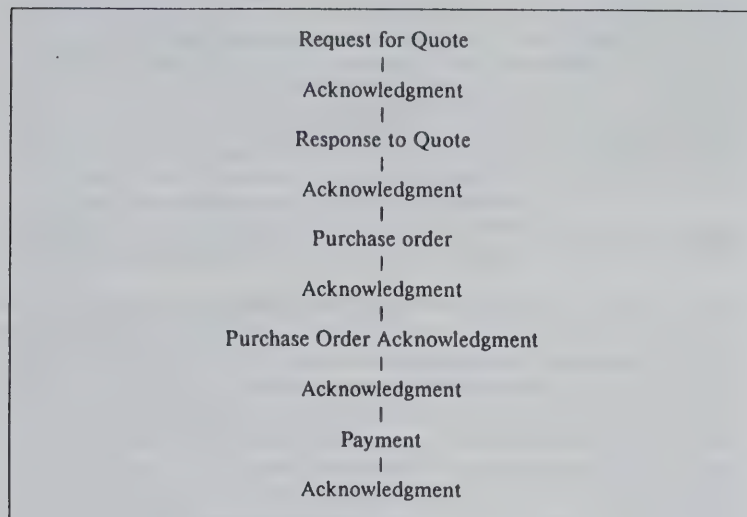


Figure 5-10. Transaction set for purchasing and payment.

proposal for a default set of transaction sets is intended to bolster open trading by increasing the reliability and certainty with which EDI could form enforceable relationships without the need for the usual implementation, or *bringing up*, process between two specific trading partners. One EDI pioneer has proposed:

[t]he development of recommended (not mandatory) *core usage*. Under this concept, persons working on an industry's usage conventions would specify a core set of conventions that would be expected to accommodate most, say 95%, but not all needs. Industry participants would be encouraged to employ the core usage conventions wherever possible, while being allowed to go outside these conventions (while staying within the regular conventions and standards) when necessary.

If core conventions can make it practical to automate the processing of most, say 95%, of all messages, we have really achieved something—the ability to automate the routine bulk of the workload and to focus our manual attention on the special and unusual.<sup>168</sup>

Clearly, default transaction set series could not satisfy all trading needs. However, they could help to rationalize testing, and to make sophisticated interoperability testing (of, for example, transaction flow) more viable.

<sup>168</sup> *Id.* at 102-03 (emphasis added).

### § 5.36 —The Clearinghouse and Testing

An EDI clearinghouse could play an important testing role by providing a limited set of testing-related services, such as (1) identifying selection criteria, (2) developing and maintaining a list of software vendors (a Better Business Bureau-like role), and (3) working with industry groups to develop industry-specific testing regimes. A prospective trading partner could be certified upon passing a clearinghouse testing regime.<sup>169</sup> A clearinghouse agreement could impute predetermined legal significance to the certification. For instance, trade transactions executed over an interoperability certified system could be presumed accurate and enforceable. Thus, when a certified trading partner sends an electronic order to a vendor, the parties would be estopped from denying the authenticity or integrity of the order unless probative evidence demonstrates otherwise.

Trading partners could also privately agree that certification evidences an implementation's "commercially reasonable" security when, for example, testing of cryptographic or other security mechanisms is undertaken. Trading partners could accordingly establish an agreement that apportion liability for erroneous transactions in some cases. Commercial law provisions apportion liability in accordance with the use of security procedures.<sup>170</sup> Certification might also be used as a prerequisite to obtaining or maintaining EDI insurance coverage,<sup>171</sup> reducing EDI insurance

<sup>169</sup> There could be more than one testing level or regime, and each regime could provide (and the parties could legally impute) a different degree of reliability, strength, and/or trustworthiness to such certification. A special code (for example, in a data element) could be assigned to each level of certification and be included in EDI messages, trading partner profiles, or clearinghouse databases. See *Pedi* conformance requirements in CCITT Message Handling: EDI Messaging Service Draft Recommendation F.435, cl. 21 (1990).

<sup>170</sup> For example, U.C.C. art. 4A § 202(b) apportions liability based on the use of a security procedure:

If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedures and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer (emphasis added).

<sup>171</sup> While system-perils insurance policies (e.g., by Lloyds of London) and generalized data processing umbrella insurance policies are available, they do not specifically address electronic contracting. This area is fertile ground for insurance industry consideration and development.

premiums, or communicating sensitive or proprietary information between trading partners.<sup>172</sup>

As a primary testing entity, the clearinghouse could serve as a repository for current standards and industry implementation guidelines, as well as for documents maintained by government or standards entities.<sup>173</sup> This could ensure that clearinghouse testing regimes are accurate and current and provide real-time information to nonconforming users, such as those who failed interoperability testing, to help them obtain compliance.

The clearinghouse could also participate in establishing performance criteria and testing. "In government contracting, the acquisition authority must determine and specify those performance-related features that are desired to be under user or application process control and those desired to be under system operator control. The [parties] . . . may also wish to specify benchmarking criteria as evidence of satisfying performance requirements."<sup>174</sup>

A clearinghouse could provide for the registration of critical specifications for industry, such as the actual data length requirement by data elements and the required presence of optional data elements. Having access to such specifications could provide a tangible boost to error-free enablement and migration activities in EDI.

Standards for clearinghouse-related interoperability testing accreditation could potentially be developed in conjunction with, or partially modeled after, the National Institute of Standards and Technology's (NIST) National Computer Standards Laboratory (NCSL). NCSL is responsible for interoperability certification of diverse computer and telecommunications equipment. Its National Voluntary Laboratory Accreditation Program (NVLAP) was established to facilitate the accreditation of private laboratories that perform specific testing, including conformance testing,<sup>175</sup> and is a useful

<sup>172</sup> Approval of a security implementation prior to its use in the communication or storage of government secrets provides precedent for commercial certification as a prerequisite to the electronic communication of proprietary trade secrets.

<sup>173</sup> For example, the X12 EDI database contains all standards published by the Data Interchange Standards Association (DISA) (including all version releases). The database is maintained by DISA. In contrast, the UN/EDIFACT standards database is not centrally maintained, nor is it maintained with a comparable level of integrity. See Minutes of the Ad Hoc Team on Data Base Coordination, UN/ECE TRADE/WP.4 (Geneva Dec. 13, 1990) (representative from ISO presented a plan for on-line access to ISO information, ISONET). Perhaps this could lead to on-line UN/EDIFACT standards information. The clearinghouse could help to rationalize UN/EDIFACT standards maintenance on behalf of the clearinghouse user community.

<sup>174</sup> FIPS PUB 146 at 12.

<sup>175</sup> See 15 C.F.R. § 7 (1990). National Institute of Standards & Technology, NVLAP Program Handbook, Computer Network Interface Protocol X.25, Doc. No. NISTIR 89-4036, at 3 (Mar. 1989). "NVLAP offers accreditation for specific test methods or types of tests in many areas. NVLP provides an unbiased third party evaluation and

model for the development of building blocks supporting clearinghouse electronic trade testing.<sup>176</sup>

NVLAP procedures for the accreditation of laboratories include detailed requirements for on-site assessment by NIST; meeting with laboratory managers; examining quality assurance systems; producing documentation; running samples; reviewing personnel records and records of periodic internal audits; observing demonstrations of testing techniques; and examining major equipment, apparatus, and facilities. Already, NIST has adopted a federal information standard for EDI.<sup>177</sup> This standard incorporates the data communication protocols defined in Federal Information Processing Standard Publication 146 (GOSIP).

The clearinghouse could potentially serve as a primary NIST accredited conformance testing site. However, it is unlikely that NIST can soon focus sufficient resources on developing EDI conformance testing, because NIST is constrained by limited resources, or "resource bound." The European Community has taken a strong position on EDI certifications that has not been recognized by United States testing entities.

The increasing complexity of electronic trade transactions, the need to bring up many trading partners, the existence of open trading requirements, and the desire to eliminate paper hasten the need and provide the opportunity to implement and utilize sophisticated testing. However, to be useful, testing must be thoughtfully implemented, work properly, yield significant results, and be accepted by the electronic trading community.

## § 5.37 Contract Determinative Services

Determining whether and when trading partners have reached an agreement and what constitutes the agreed-upon terms are classic contract law

recognition of performance as well as expert technical assistance to upgrade laboratory performance." See also 35 Fed. Reg. 410, at 27,543 (July 21, 1988).

<sup>176</sup> NVLAP accreditation signifies recognition of a testing laboratory's competence to perform specific test methods in specified fields of testing. It means that the laboratory's quality system, staff, facilities and equipment, calibration procedures, test methods and procedures, records, and test reports have all been evaluated and found to meet NVLAP criteria. NVLAP accreditation does not mean a guarantee (certification) of laboratory performance or of product test data; it is solely a finding of laboratory competence. . . .

. . . Accreditation does not relieve the laboratory of the need to observe and comply with existing Federal, State, and local statutes, ordinances, or regulations that may be applicable to its operations, including consumer protection and antitrust laws.

NVLAP Program Handbook at 3.7.

<sup>177</sup> See Ch. 4 on GOSIP.



problems that affect both conventional and electronic contracting. Resolution of these problems is not simple and may be further obfuscated by the novel issues and complexities attendant to electronic contracting.<sup>178</sup> In electronic contracting, a description of the goods and services is sent electronically, while the underlying terms and conditions are typically communicated by conventional (paper) means, such as in a trading partner agreement (TPA). This bifurcation in EDI of the description of the goods and services from other terms and conditions is a potential impediment to contractual certainty. Nonetheless, the communication of information in a more standard fashion via EDI standard formats can simplify contract certainty.

Contract Determinative Services (CDS) are intended to facilitate the automatic review of EDI transactions in order to determine if and when a contract was created, its contractual significance, the contract's terms and conditions, and the existence of any responsive obligations.<sup>179</sup> Each of these issues calls for definitive legal solutions—however, certainty is not generally available. The variety of legal requirements applicable to each situation may hinder definitive determinations. However, various technologies and procedures can provide useful inferences about the meaning and contractual significance of EDI information and help to process it intelligently. A clearinghouse can provide such CDS services, as demonstrated in the following examples.

#### Problem 1—Contract Tracking

A customer sends a material release<sup>180</sup> to a vendor for the purchase of subassemblies (component parts) used in a just-in-time manufacturing

<sup>178</sup> See Savage, *Discussion Paper on Negotiating EDI Terms and Conditions*, EDI Committee Meeting Materials, 1990 A.B.A. Sec. Sci. & Tech.

<sup>179</sup> CDSs are not necessarily best implemented in a clearinghouse, and some aspects of CDSs are currently implemented with trading partners' EDI and application systems.

<sup>180</sup> For example, the draft proposed X12.14 Planned Schedule with Release Capability Transaction Set (830):

[p]rovides for customary and established business practice relative to the transfer of forecasting/material release information between organizations.

The planning schedule transaction may be used in various ways or in a combination of ways, such as: (1) simple forecast; (2) a forecast with the buyer's authorization for the seller to commit to resources, such as labor or materials; (3) a forecast that is also used as an order release mechanism, containing such elements as recourse authorizations, period-to-date cumulative quantities, and specific ship/delivery patterns for requirements that have been represented in "buckets," such as weekly, monthly, or quarterly. The order release forecast may also contain all data related to purchase orders, as required, because the order release capability eliminates the need for discrete generation of purchase orders.

environment. Under the terms of a master agreement, the subassemblies must be delivered within 45 minutes of the time they are ordered. The subassembly vendor duly sends an electronic ship notice to the customer<sup>181</sup> indicating that the shipment will be delayed.

CDS implemented within a clearinghouse could monitor the transmissions in relation to the terms of the master agreement. The CDS could immediately notify the customer of the time discrepancy and help the customer to determine quickly whether the vendor has breached the master agreement and, if so, what response to make in order to (1) properly notify the vendor of his alleged breach, (2) object to the delivery delay (to preserve his rights), (3) take requisite remedial action, such as to order replacement subassemblies from an alternative supplier, (4) cancel the order with the vendor, and/or (5) notify the requisite departments of the delay and likely implications to the business and manufacturing functions.

#### Problem 2—Use of Free Text

A customer orders goods from a vendor. The purchase order includes *free text*—unstructured, non-machine-processible text—which states that "We may want the right to make payment five days late." Provided the free text is considered an integral part of the contract,<sup>182</sup> how can the free text best be processed and made binding in an automated environment geared towards structured data?

Compelling and practical reasons may exist for communicating unstructured and unformatted information such as free text on an EDI communication system. EDI transaction sets and messages cannot: (1) always remain current and consistent with business practices; (2) anticipate and satisfy all business needs; (3) necessarily facilitate negotiations; (4) create

<sup>181</sup> For example, the draft proposed ANSI X12.10 Ship Notice/Manifest Transaction Set (858):

provides the standardized format and establishes the data contents of a ship notice/manifest transaction set. A ship notice/manifest lists the contents of a shipment of goods as well as additional information relating to the shipment, such as order information, product description, physical characteristics, type of packaging, marking, carrier information, and configuration of goods within the transportation equipment.

<sup>182</sup> Some TPAs provide that free text will have no legal effect. This clause is designed to achieve greater transactional certainty and to discourage the use of free text. See Ch. 2. The problems with free text arguably extend beyond its lack of machine processibility to rather technical-legal concerns regarding the legal weight properly accorded free text. An analog to free text, hand-written additions or modifications to a conventional typed document (interlineations), may be afforded more legal weight than the typed portion of the document. This traditional legal approach may directly conflict with the EDI community's intention to make machine-processible EDI data more legally binding than free text.

the psychological impact of human "colorful and persuasive writing," strategy, or maneuvering; or (5) satisfy the temporal ordering of business commitments.

Unstructured free-form text is often used for want of a conventional format to accommodate free text within existing EDI standards. Specific segments and data elements evolve over time to facilitate the communication of needed information, but all needs cannot be satisfied. For example, X12 Data Element 560 (Special Services Code) includes more than 100 special codes of specialized applicability. These codes include alterations, adjustments, bad debt, cartage, deposit, discount, delivery, early-buy allowance, engraving, gas pressure, installation, loan fee, pickle and oil, pulling eyes, shotblasting, telephone charge, and drop yard. Because it is impossible to create codes to anticipate and satisfy all business needs, there will always be a need to communicate data concerning unique business situations outside of existing EDI standards. Thus, alternative, nonconventional EDI methods to make non-machine-processible information understandable by computers are needed. A common business communications protocol (CBCP) is one such tool.

Current EDI standards recognize the need for free-form communication but discourage its use and accordingly do not provide the tools to process this form of information intelligently and expediently. Perhaps the primary obstacles are the limitations of current EDI implementations, which fail to facilitate the meaningful processing of free text.

An X12 Note/Special Instruction (NTE) segment "transmit[s] information in a free-form format, if necessary, for comment or special instruction."<sup>183</sup> The standards state that "[t]he NTE segment permits free-form information/data which, under ANSI X12 standard implementations, is not machine processable. *The use of the 'NTE' segment should therefore be avoided, if at all possible, in an automated environment.*"<sup>184</sup> The NTE segment appears in at least 23 transaction sets and is widely used, despite the official comment discouraging its use. Other X12 segments that permit free-form information should be used with caution.<sup>185</sup>

<sup>183</sup> X12 Standards, Draft Version 3, Release 1, Doc. No. ASC X12S/90-850, at 34 (Dec. 1989).

<sup>184</sup> *Id.* (emphasis added). "The use of the [Text] transaction set [(864)] to transmit quasi or unique transaction set standards is [also] discouraged." *Id.* at 67. The clearinghouse will also need to consider the legal interrelationships of various contractually significant services and document types.

<sup>185</sup> These include: K3 (File Information), which is used "to transmit a fixed format record"; MSG (Message Text), which provides "a free form format that would allow the transmission of text information"; PID (Product/Item Description), used "to describe a product in coded or free-form format"; and PKG (Marking, Packaging, Loading), which describes "marking, packaging, loading and unloading requirements." Data Element 352 (Description), which is used in the PKG segment, is a "free-form description to clarify the related data elements and their content." X12 Standards, Draft Version 3, Release 1, Doc. No. ASC X12S/90-850.

The use of the NTE or other free-text segments can result in various problems, including incomplete transaction set processing or resolution in the absence of human review, free text loss (or misplacement), and legal uncertainty.<sup>186</sup> For example: Company A sends Company B a purchase order transaction set for five computers and includes a NTE that says, "You must ship these computers in waterproof boxes." Company B receives the order and either (1) the order is delayed because of the inclusion of free-form text (because the transaction set within which the NTE appears is held in suspense until a human reviews the NTE) or (2) the order is processed but the NTE is ignored or is not effectively matched to the transaction set and delivery is made without waterproof boxes. Following delivery and inspection, Company A rejects the order due to nonconformance with the purchase order.

Regardless of the result, better facilitation and predictable treatment of free-form text is needed. Although implementation conventions and guidelines, TPAs, and trade practices provide some guidance, clearinghouse technical structures that permit the incorporation and processing of free-form text deserve consideration.

Compound documents may create comparable issues. Compound documents are created electronically by integrating elements stored in one or more networks or formats. The formats may include text, graphic images, or tables. Compound documents are frequently used for on-line electronic ordering from a catalog. Compound documents may consist of pointers to information stored in files independently maintained and updated by diverse entities. Consequently, the elements that create the document are not necessarily under the exclusive control of the document's creator, which raises interesting legal issues bearing on the ownership, accuracy, and proof of creation and modification of the documents.<sup>187</sup>

### Problem 3—General Contract Interpretation

A customer orders 500 machines from a vendor. The vendor appears to accept the order for the 500 machines by sending a purchase order acknowledgement<sup>188</sup> to the customer, but the vendor adds additional terms

<sup>186</sup> The extent to which a note should be considered legally binding is unclear in the absence of express TPA provisions.

<sup>187</sup> See, e.g., *Electronic Messaging*, A.B.A. Report No. 507-0210 (1988) 22 (discussion of hypermedia). Also, new "three dimensional tools" for organizing information have been developed. It is recognized that "with any of this technology you need additional clues as to where you are." Andrew Pollack, "Coming Soon: Data You Can Look Under and Walk Through" at 9 (Oct. 14, 1990) (quoting Will Kessler).

<sup>188</sup> See X12.9 Purchase Order Acknowledgment Transaction Set (855), which "provides for customary and established business and industry practice relative to a seller's acknowledgment of a buyer's purchase order."



requiring that the machines be shipped by a named shipper. Is there a contract? And, if so, what are its terms?<sup>189</sup>

To address these problems, the clearinghouse CDS could include a CBCP.<sup>190</sup> A CBCP may also alleviate free-text problems, such as in Problem 2, and contributes to a framework for contract interpretation. This is accomplished by (1) making unstructured and unformatted text amenable to machine interpretation and (2) providing for a human-readable dialog, perhaps in real time. A CBCP may also provide semantic access to the information—that is, access to its meaning.<sup>191</sup> CBCP uses a variable structured format that allows machine processing within the flexibility of free text.

CBCP messages are lists of items punctuated by parentheses. The lead item of each list identifies the type of message and is used to determine how to interpret the rest. The items may be either sublists or atoms. If an item is a sublist, its first element tells how to interpret it. . . . No position should require an identifier or a number per se but should allow a phrase. . . . The following . . . is an example of CBCP: (REQUEST-QUOTE (YOUR-STOCK-NUMBER A7305) (UNITS 100)).<sup>192</sup>

A CBCP could be used by trading partners to bridge the gap between free text and highly structured data. A CBCP language and an interpreter could facilitate the use of a limited English-language dialog in an otherwise unstructured message within the EDI transaction sets. A CBCP might also

<sup>189</sup> Of course, this is a problem affecting not only EDI. However, to the extent that EDI requires greater transactional certainty and speed, the clearinghouse could provide value in attempting to mitigate these problems.

<sup>190</sup> See McCarthy, *Common Business Communications Language*, in Textverarbeitung und Buerosysteme (A. Endres & J. Reetz eds. 1982), cited in Cohen, *Electronic Commerce*, ISI Research Report ISI/RR-89-244, at 23 (Oct. 1989). The CBCP is inherently flexible; the structure of each message is defined by the user. This flexibility sharply contrasts with the rigidity of EDI standards that attempt to predefine all aspects of message format, syntax, and structure. EDI standards can rarely define all such structures in a timely or sophisticated fashion.

<sup>191</sup> Kimbrough, Reddi, & Thornburg, *On Messaging with Semantic Access in an Office Environment*, Coast Guard Contract DTCG39-86-C-80348, at 2 (Dec. 1989). Kimbrough asserts that "EDI message formats will eventually need to be based on expressions in recursively-defined formal languages . . . [based on] formal languages for business communication." S. Kimbrough, *Brief Statement on EDI Research and Development Interests* (May 15, 1990). In general, Kimbrough views current EDI problems as those of message management:

[M]essage management software should be designed so that any operation . . . upon a message may be expressed in a declarative language built for this purpose. This done, the message management software should be able to interpret the declared expressions—in the context of the messages and the organization's data processing system—in order to effect the intended operations.

Kimbrough at 4.

<sup>192</sup> Cohen, *Electronic Commerce*, ISI Research Report ISI/RR-89-244, at 26 (Oct. 1989).

complement, or provide structural underpinnings for, generic transaction sets or messages.

A CBCP and other CDSs could enhance EDI system translation, as well as interpretation, tracking, and interrelationships among: underlying business terms and conditions, master contracts, industry and proprietary implementation guidelines, EDI TPAs, trading partner profiles, other contractually significant documents, statutory and case law,<sup>193</sup> and the EDI transactions themselves. CDS could logically extend validity checks to both profile and conditional information.<sup>194</sup> Although there is increased excitement about these developments, such state-of-the-art procedures are "best described as being in the exploratory phase."<sup>195</sup>

Figure 5-11 represents the relationship of some of the services and document types that clearinghouse CDSs may provide.

A CDS may include *performative*<sup>196</sup> contract capabilities intended to directly affect the legal relationship of both structured and nonstructured communications. The *performative network*, on which electronic contracting is executed, is a fairly new concept. The term underscores the differences between electronic contracting and the activities supported by conventional communications networks, which are described as *informative networks*. Informative networks are meant to expedite data transfer. How the transferred data is subsequently used and how it changes the state of affairs is not the concern of informative networks. Performative services provide expert/intelligent system capabilities that support greater automation and may alleviate free-text problems. They may also permit the clearinghouse to improve "exception handling" automation.

<sup>193</sup> Westlaw developed a prototype system to automatically update contracts based on changes in the law. Westlaw subsequently dropped that project because of its complexity and the problems inherent in automatically interpreting the law. A program of this magnitude may be premature compared to the focused, less ambitious use of the tools discussed in this chapter.

<sup>194</sup> EDI transaction sets currently provide some constraining variables of contractual significance. For example, the X12 CSH (Header Sale Condition) segment, which is used to specify general conditions or requirements of a sale, includes a data element "Do-Not-Exceed Amount" and related conditionals. Additionally, trading partner application profiles are maintained within trading systems, within underlying business applications, and by TPSPs. They include the data sets created in anticipation of electronic trading and are not limited to information identifying a trading partner's name, permissible transaction sets, authorized representatives, dollar and quantity minimums/maximums, and other information associated with basic trading parameters.

<sup>195</sup> Kimbrough, Reddi, & Thornburg, *On Messaging with Semantic Access in an Office Environment*, Coast Guard Contract DTCG39-86-C-80348, at 8 n.173 (Dec. 1989).

<sup>196</sup> Performatives and performative networks are described in Dewitz & Lee, *Legal Procedures as Formal Conversations: Contracting on a Performative Network* (July 1989). *Performative speech acts* are distinguished from *informative speech acts* in that the former have direct legal impact and the latter convey information without legal impact. Cf. functional versus informational messages in Ch. 11.

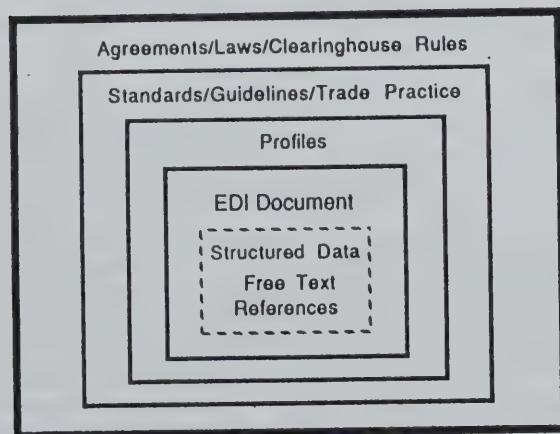


Figure 5-11. CDS services/document types.

### § 5.38 —Standard Generalized Markup Language

An example of a performative-like structure employed in electronic publishing is the Standard Generalized Markup Language (SGML). SGML prescribes the construction of grammar for structured documents, both linguistically and mathematically, for the formatting, presentation, and transfer of documents between computerized systems. SGML also can be incorporated to address those issues related to the parsing of free text in EDI documents. SGML was developed by the International Organization for Standards (ISO) to automate publication procedures. The grammar developed under SGML guidelines defines a language that marks up, or *tags*, text according to its meaning or purpose. Both the text and the tags, such as “<chapter>,” are machine-readable. Tags are used to denote the starting of a structural element, and an end tag, such as <chapter>, identifies the end of the structure.

One purpose of marking up text by SGML is to automate the document's printing. Because the machine can recognize each functional element of the text once it is marked up by SGML, the instructions to the printer can be separated from the text itself and contained in an electronic style sheet. The instructions to the printer specify how each functional element, for example, the bibliography or the abstract, should be presented. And, if it is later determined that the text must be presented in another form, only the electronic style sheet need be changed to modify the format throughout the entire document.

Two principal advantages of SGML render it applicable to electronic contracting, *generality* and *extensibility*. Generality refers to SGML's treatment of each document as a hierarchy of data elements and marks up the role of the elements irrespective of their contents. It can handle all kinds of structured or unstructured documents, including the free text of an EDI document. In operation, the preparer of an EDI document that requires the use of free text (that is, a document for which existing standards encoding is inadequate to concisely communicate the intended information) could mark up the free-text portion of the document with SGML according to predetermined legal or business conventions for each operative word or phrase. Software could be designed to facilitate and expedite this procedure. Once marked up, the document's free text becomes highly machine-readable. The software interpreter that verifies the document structure could also be modified to accommodate changes in the law. A function of the interpreter is similar to that of the electronic style sheet: by changing the electronic style sheet the presentation of text is changed.

SGML's extensibility bolsters its relevance to EDI and electronic contracting. SGML can be viewed as a set of opening and closing tags used to delimit specific functional elements. For example, there may be one set for the glossary and one for the bibliography. In practice, however, there may be various functional elements that do not have a predefined tag. In such a case, one need only add a new tag to support the omitted functional element. Such flexibility is referred to as extensibility because the language can be extended readily to accommodate modern needs. The minimum tag set for a document may encompass just one tag, such as <edidoc>, to indicate the start of the document with an assumed end tag, <edidoc>, to close the document. Others may require that just a few elements be tagged. Finally, there may be some critical documents that must have all elements tagged so that a more intelligent search and processing of the document contents can take place.

The idea of an SGML-like language as a solution to the free-text problem in electronic contracting represents an attempt to take advantage of SGML's duality. Because this approach provides for new uses of documents, it will be almost impossible initially to categorize all the data elements according to their legal and administrative functions. Rather, the classification periodically will need to be extended through the addition of tags or modification of document structures. The extensibility of SGML allows for the use of methods to update and process large volumes of documents automatically by setting global style definitions which can be implemented in an automated processing system. This avoids the expense of manually updating documents as is done in desktop publishing.

The guidelines of SGML do not actually define tags to be used in EDI documents, but they do provide a foundation upon which to base a set of tags for EDI documents. It falls to the EDI community to determine the



document structures and the appropriate tags to be used to identify the structure within a document. The nature of EDI documents indicate that some tags should be dedicated to document structure and others should indicate key contractual elements content. A rich set of tags that identify important components of a contract's structure and content will provide for most needs of the EDI community. Contract terms and conditions might be a good pilot. Unique contractual requirements and free text could be provided for through the use of broad usage tags, such as <note> or <specification\_item>.

EDI documents are generally required to be created according to EDI standards, such as UN/EDIFACT or ANSI X12. The drawback to this approach is its inflexibility: it would impose too much constraint on trading partners. Some business documents cannot be categorized into any one of the preexisting transactional sets. The coexistence of structured and unstructured EDI documents would greatly alleviate such constraint. An SGML-based but EDI-specific grammar can exploit the existing technology to grapple with the unstructured EDI documents without undue complication from modification of current ISO SGML. It also provides a mechanism to deal with multimedia documents and provides a path to unforeseen future requirements.

For example, suppose that a purchase order is created that incorporates free text and is also marked up by some SGML-like language. How would an automated processing system find out the destination to which the ordered commodity is to be shipped? It would first try to find the start- and end-tags for *carrier details*. Once those elements are found, the machine would then try to locate within the carrier details element another tag set for *geographical location*. The destination could then be located within the last pair of tags for geographical locations. All of the text in the example described could be machine processed but also humanly readable.

For an example of unavoidable free text, consider a conditional purchase order. Suppose Party A wants to buy an item from Party B, but only after Party B can make explicit statements about certain attributes of this item. Party A intends to send a message that would be recognized as a purchase order for an item by Party B, if Party B can send a message back to Party A confirming that the item has certain attributes. The return message with confirmation then would be recognized as a purchase order acknowledgment by Party A. Both Party A and Party B want those messages to carry contractual obligations. ANSI X12 standards cannot handle such EDI documents because neither the conditional purchase order nor the conditional acknowledgment is expressly and richly provided as a standard transaction set. In such cases a combination of free text and SGML-based EDI grammar to tag the free text would be very useful.

There is a need to eliminate ambiguous wording within the free text or notes of a contract. Ambiguity could be damaging in, for example, an

agreement between a landscape contractor and a client during the development of a project. If the agreement is for the contractor to provide grounds maintenance for the "length of the project," the contractor may assume that the length is "500 feet" as previously discussed, while the client assumes that the length is the summer months "May to August" as previously discussed. Some documentation professionals are working to develop *simplified English* requirements that incorporate a core of common English words and a minimum of technical terms based on the core words for definitions. Similar efforts are underway in other countries for simplified French, Spanish, and Japanese.

While SGML offers a useful foundation, a new EDI formal grammar is needed to meet the documentation needs of the contracting community. In addition, a natural-language grammar is needed to facilitate the wording of free-text notes within a contract. This new grammar would eliminate slang, regional usages, individual quirks, and ways of expressing ideas. One final benefit of a new natural-language grammar is that it would facilitate language conversion and therefore promote international usage. Unfortunately, this may ignore the root problem: The data to be encoded in CBCP or SGML cannot be fully processed by the application, even if the EDI system can decode it. This is a profound problem that only time will heal. EDI has begun to change business systems, and that evolutionary process will take time before success with alternative approaches can be realized.

SGML is certainly not the only technology adaptable to EDI documents. Other developing standards for document interchange may soon become available to electronic contractors. Government agencies, including the United States Navy as well as other industry standards organizations, particularly the International Telephone and Telegraph Consultative Committee (CCITT), have actively worked in this area for many years. Another document structure approach is based on the ISO standard Office Document Architecture (ODA),<sup>197</sup> which is finding use in consumer and office network systems. Similarly, IBM Corp. has created including its Document Content Architecture (DCA) to address the syntactic issue.

### § 5.39 Clearinghouse Regulatory Considerations

The remainder of this chapter examines important clearinghouse regulatory issues that primarily concern antitrust principles and restraint of trade, as they relate to the clearinghouse. A summary of related telecommunications regulatory considerations also is presented, followed by a discussion of the clearinghouse's role in the standards-making process.

<sup>197</sup> ODA is being proposed as an encoding format for use in multimedia mail and file exchange within Internet. ODA is defined in ISO 8613.

### § 5.40 —Antitrust Considerations

Antitrust laws are designed to promote competition in open markets, in part by proscribing unlawful restraints of trade and unfair business practices. The clearinghouse's role as an intermediary in business transactions raises actual or perceived antitrust issues, including: whether clearinghouse implementation could result in or be viewed as a concerted refusal to deal with trading partners who do not use the clearinghouse or with TPSPs who do not interconnect with the clearinghouse, whether clearinghouse activities and rules confer an illegal competitive advantage upon clearinghouse users, upon third parties who interconnect with the clearinghouse, or even upon other prospective clearinghouses, and whether clearinghouse implementations create price-fixing problems. Section 5.41 considers the application of essential facilities doctrines and § 5.42 addresses joint venture issues.

### § 5.41 —Essential Facilities Doctrine

A limited number of clearinghouses, or perhaps only a single clearinghouse, will exist in any given market. Whether a clearinghouse is deemed to constitute an essential facility will affect the business activities of clearinghouses and the extent of governmental regulation under the antitrust laws.

The existence of competing clearinghouses would provide users with alternative facilities. The existence of effective substitutes would render inapplicable the essential facilities doctrines. Because each clearinghouse would be an effective substitute for the others, a determination that any one clearinghouse constitutes an essential facility would be precluded.<sup>198</sup> The following arguments would also support this conclusion:

1. Control is not in the hands of a monopolist when the clearinghouse is an appropriate joint venture and is operated with fairness, participation, and nonexclusivity.
2. The availability of technology for the interconnection of resources permits competitors to duplicate clearinghouse facilities. Moreover, available open systems technology makes redundant or competing clearinghouse facilities more feasible.<sup>199</sup>

<sup>198</sup> *In re Air Passenger Computer Reservation Sys. Antitrust Litig.*, 694 F. Supp. 1443, 1455 (C.D. Cal. 1988).

<sup>199</sup> *Id.* at 1453-56 (effect of entry barriers to market competition on the finding of an essential facility).

3. The clearinghouse can and should be made available to competitors. Many clearinghouses have been successful in including competitors.<sup>200</sup> It is important to note, however, that under antitrust principles "absolute equality of access" is not required by the Sherman Act.<sup>201</sup>

### § 5.42 —Clearinghouse as Joint Venture

This section discusses the application to clearinghouse joint ventures of two alternative doctrines ancillary to the Sherman Act. The *per se* doctrine and the rule-of-reason doctrine are two alternative tests under which to gauge whether an anticompetitive activity is a violation of the Sherman Act. For a detailed explanation of these doctrines and the Sherman Act, see Chapter 10. Electronic trade clearinghouses will increasingly be owned or operated by a consortium of companies, industries, and organizations. When a clearinghouse is classified as a joint venture, the weight of authority holds that allegations about clearinghouse price fixing would not be evaluated under the *per se* rule, but instead under the rule of reason analysis.<sup>202</sup>

The Supreme Court has voiced a preference for the application of the rule of reason in new industries with clearinghouse-like attributes: "The bank card industry is a relatively new one and . . . a very large and important segment of our economy. Considering the importance of the industry and the lack of definitive information relating to competition therein, it would be a mistake to determine this case of first impression on a *per se* basis."<sup>203</sup>

Joint ventures can encourage innovation and provide services that otherwise would not exist.<sup>204</sup> Arguably, even if clearinghouses function as separate corporations rather than as actual joint ventures, the necessary interrelations could lead to application of joint venture principles. In a VISA bankcard case, the court found that the evidence pointed to a complex set of interrelationships between cardholder and merchant that suggested the

<sup>200</sup> For example, Baxter Healthcare Corporation's ASAP Express (§ 5.4), or the WORLDSPAN airline reservation system (§ 5.7).

<sup>201</sup> And its feasibility and practicability are only additional considerations.

<sup>202</sup> *National Bancard Co. v. VISA, U.S.A., Inc.*, 596 F. Supp. 1231, 1252 (S.D. Fla. 1984).

<sup>203</sup> *Id.* at 1255 (quoting *Worthen Bank & Trust Co. v. National BankAmericard, Inc.*, 485 F.2d 119 (8th Cir. 1973), *cert. denied*, 415 U.S. 918, 94 S. Ct. 1417, 39 L. Ed. 2d 473 (1974) at 129-130).

<sup>204</sup> See *Cooperative Research—Antitrust Aspects Trade Reg. Rep. (CCH)* § 50,411 (speech by P. Ewing Jr., Deputy Assistant General, Antitrust Div., Feb. 19, 1980).



presence of a joint venture—even though VISA could not properly be characterized as a joint venture in the strictest sense of the word:

In VISA's case, profits and losses are not specifically shared among the various VISA members, nor is there any commingling of management functions. Furthermore, to the extent possible, each member engages as an independent unit in economic competition with other VISA members with respect to various aspects of their common venture. . . .

The fact that VISA members have integrated to the extent of agreeing on the terms of interchange, but have not fully integrated and still compete for cardholders and merchants, is typical of pro-competitive joint ventures. . . .

The principal purpose of these agreements . . . does not appear to be to improperly fix prices . . . but rather to provide a service which each member bank could not alone provide.<sup>205</sup>

### § 5.43 —Telecommunications Regulatory Issues

As providers of services relating to telecommunications, clearinghouses may be subject to state and federal regulation. The extent of telecommunications regulation applicable to clearinghouses largely depends on the scope of services provided. If clearinghouse activities resemble the provision of data-processing services, fewer regulations will apply. To the extent that EDI services resemble common carrier basic services (or nonenhanced or non-value-added services), there will be more regulatory considerations. Furthermore, because domestic United States and non-United States<sup>206</sup> regulatory concepts are not identical, geographical differences in the scope of telecommunications regulation may affect some clearinghouse functions.

**Structural regulation.** The FCC has authority to regulate interstate communication services by wire or radio.<sup>207</sup> Intrastate communications are left to state regulation.<sup>208</sup> Because clearinghouses provide for the transfer of information and communication mechanisms between contracting parties, they would fall within the authority of the FCC and the state regulators.

<sup>205</sup> National Bancard Co. v. VISA, U.S.A., Inc., 596 F. Supp. 1231, 1253–54 (S.D. Fla. 1984) (emphasis added).

<sup>206</sup> International communications is one of the fastest growing segments of the U.S. telecommunications industry according to the FCC. *Trends in the International Telecommunications Industry 1975–1988* (Dec. 1989). Revenues were reported rising from \$862 million in 1975 to \$3.4 billion in 1988, with an annual growth rate of 25–30%.

<sup>207</sup> 47 U.S.C. § 151 (1988).

<sup>208</sup> 47 U.S.C. § 152(b)(1) (1988).

The FCC has decided not to regulate “enhanced services,”<sup>209</sup> such as data transfers, but rather to promote competition in the industry.<sup>210</sup> However, because these services use the transmission facilities of common carriers, they are affected by FCC regulation. Basic service providers, principally the regional Bell Operating Companies (BOCs), are required to provide enhanced services through a separate subsidiary. This requirement serves to separate the regulated and unregulated parts of the company and prevent cross-subsidization.<sup>211</sup> The structure of the clearinghouse could serve to classify the service as a common carrier rather than solely as an enhanced service.<sup>212</sup> Common carriers provide data transfer services to all who apply, at common carrier rates. Common carrier regulation restricts the variety of services that can be provided, requires certain levels of service and performance to be maintained, and sets rates that can be charged. Even if clearinghouses were considered common carriers, the imposition of extensive regulations is unlikely because the FCC has been more lenient in regulating non-BOC carriers. For example, GTE has been excluded from BOC regulations despite providing both basic and enhanced services.<sup>213</sup>

Another area of FCC regulation that would affect clearinghouse functions relates to the connections between outside services and the BOC local telephone switches. Because the local exchanges create a bottleneck in the communications systems,<sup>214</sup> significant FCC policies and regulations restrict control of the access to local exchanges and regulate their pricing. The local exchanges must provide nondiscriminatory access to all who apply. Such regulation permits easy access by clearinghouses to traditional communications facilities. However, if the clearinghouse seeks to provide alternative connections, it will be within the scope of these FCC regulations.<sup>215</sup>

<sup>209</sup> Enhanced services combine pure transmission capabilities (basic service) with “computer processing applications [that] . . . act on the format, content, code, protocol or similar aspects of the subscriber's transmitted information, or provide the subscriber additional, different or restructured information.” Final Decision, *In re* Amendment of § 64.702 of Comm'n's Rules & Regulations (2nd Computer Inquiry), 77 F.C.C.2d 384, 387 (1980).

<sup>210</sup> See *California v. FCC*, 905 F.2d 1217, 1223–24 (9th Cir. 1990) (discussion of enhanced service industry and FCC actions).

<sup>211</sup> Final Decision, *In re* Amendment of § 64.702 of Comm'n's Rules & Regulations (2d Computer Inquiry), 77 F.C.C. 2d 384 (1980).

<sup>212</sup> See, e.g., Marks, *Regulation and Deregulation in the United States and Other Countries*, Telecommunications and the Law 129, 129–145 (W. Saproonow ed. 1988).

<sup>213</sup> *California v. FCC*, 905 F.2d 1217, 1237 (9th Cir. 1990).

<sup>214</sup> A bottleneck is a monopoly of a necessary step in an industry. The local exchanges are considered the sole access to the communications system. *Id.* at 1224 n.5.

<sup>215</sup> See *Southern Pac. Communications Co. v. Am. Tel. & Tel. Co.*, 740 F.2d 980, 1007–10 (D.C. Cir. 1984) (discussing control of access to local exchanges).

and may be subject to regulatory restrictions in its dealings with customers, with respect to rates, services offered, and acceptance of all applicants.

**Economic regulation.** To the extent that a clearinghouse provides basic service, its rates would be set and adjusted by the states and the FCC. Furthermore, despite the FCC policy promoting competition in, rather than regulation of, enhanced services, the regulatory statutes provide authority for greater regulation of the whole industry. In fact, the provision of enhanced services by BOCs has been extensively controlled.<sup>216</sup>

**State versus federal telecommunications regulation.** The Federal Communications Act<sup>217</sup> creates a dual regulatory framework: the FCC regulates interstate communications and the states control intrastate elements. Generally, states regulate the rates for local telephone services and the structure of local communications companies. Courts have held that 47 U.S.C. § 152(b)(1)(1988) prevents federal preemption of state regulation for intrastate activities.<sup>218</sup> Therefore, multiple and possibly conflicting regulations could be applied to clearinghouse service providers. The relative authority of state and federal regulators over clearinghouse activities will, again, depend upon the structure and services of the clearinghouse.

#### § 5.44 Standards Participation by the Clearinghouse

Clearinghouse representatives will inevitably participate in creating and implementing technical and legal standards for electronic contracting<sup>219</sup> and serving as an industry representative for EDI users. Applicable antitrust laws mandate that the positions taken by the clearinghouse in its standards-making and advocacy role must not restrain trade. Further, clearinghouse involvement in standards-making bodies should have the effect neither of unfairly excluding users or classes of users from participating in the clearinghouse nor of excluding other clearinghouses from

<sup>216</sup> See generally *California v. FCC*, 905 F.2d 1217, 1223-30 (history of enhanced service regulation).

<sup>217</sup> 47 U.S.C. § 151 (1988).

<sup>218</sup> *California v. FCC*, 905 F.2d 1217, 1239-40 (9th Cir. 1990); *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 370, 106 S. Ct. 1890, 1899 (1986).

<sup>219</sup> Examples of such leadership by entities exhibiting clearinghouse-like attributes include NACHA and the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which are actively represented in domestic and international standards bodies; the Uniform Code Council, which is a major force within X12; and, increasingly, various government agencies such as the United States Customs Service and the DoD.

participation.<sup>220</sup> For example, within ASC X12 standards development, representatives of the Federal Reserve Board and of NACHA advocated different standards. The Federal Reserve advocated eliminating automated clearinghouse formats, whereas NACHA alleged that such a change was not supported by business usage. The net effect of its action might have unfairly constrained or diminished NACHA's clearinghouse position.

#### § 5.45 —Clearinghouse Guideline Making

Establishing viable clearinghouse guidelines is important to successful clearinghouse operation, particularly because some clearinghouse services not only are novel, but affect multiple industries and disciplines and involve transactions that are generally contract intensive. Thus, "there must be 'rules' to enable the efficient coordination of the otherwise disparate operations of . . . members."<sup>221</sup> The interrelationships among varying rules, regulations, and guidelines must be clear and well understood. For example, consider the UCC's treatment of clearinghouse guidelines:

Local clearinghouses have long issued rules governing the details of clearing, hours of clearing, media of remittance, time for return of mis-sent items and the like. The case law has recognized such rules, within their proper sphere, binding on affected parties and as appropriate sources for the court to look to in filling out details of . . . [the] law.<sup>222</sup>

Additionally, consider NACHA's Operating Guidelines, which state:

Procedures described in [the Guidelines] . . . though not mandatory, are recommended by NACHA as sound practices. Deviation from or alteration of these on the local level should be done only after careful consideration, recognizing that local procedures may be developed that conflict with the NACHA Operating Rules for processing inter-regional entries. Additional procedures not described here should also be developed locally wherever appropriate.<sup>223</sup>

Clearinghouse guidelines should describe relevant clearinghouse infrastructure, management, operations, protocols and standards, implementa-

<sup>220</sup> For a discussion of appropriate procedures for standards making, see generally *American Soc'y of Mechanical Eng'rs, Inc. v. Hydrolevel Corp.*, 456 U.S. 586 (1982); *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492 (1988).

<sup>221</sup> *National Bancard Co. v. VISA, Inc.*, 596 F. Supp. 1231, 1255 (S.D. Fla. 1984).

<sup>222</sup> U.C.C. § 4-103, Official Comment 3.

<sup>223</sup> *Preface to NACHA Operating Guidelines*, NACHA at Operating Guidelines (OG) viii (1990).



tion requirements, security, authentication procedures, and other useful information.

Finally, the clearinghouse should ensure that its protocol and equipment requirements can interconnect with available and widely used protocols and equipment and that such requirements are neither unduly sophisticated nor unnecessarily discriminatory against certain vendors of equipment or technology.

### § 5.46 —Overcoming Regulatory Road Blocks

Policies and actions relating to antitrust law that should be considered in implementing or arranging to use a clearinghouse include the following:

**Accessibility.** The clearinghouse should be available to users on a nondiscriminatory basis. All users, regardless of size, should benefit from the clearinghouse.

**Technology and equipment.** Technology and equipment specifications should not unduly discriminate against users, manufacturers, or providers. The clearinghouse should take reasonable steps to accommodate the broad and generic use of available technologies.

**Clearinghouse rules.** The rules should expressly state the purpose of the clearinghouse, ensure its legality, and provide for fair and lawful application of its rules.

**Architecture.** The clearinghouse should be structured to support vertical market activities; it should ensure that it is not used as a price-fixing tool.

**Preclearance procedures and advisory opinions.** It may be advisable to review the permissible preclearance procedures in the Justice Department's Business Review Procedures<sup>224</sup> or in an FTC advisory opinion.<sup>225</sup> Establishing a liaison to the FTC and Justice Departments should be considered to keep them apprised of clearinghouse status and plans.

**Data policy.** A clearinghouse data policy should expressly state how the clearinghouse will provide for trade data confidentiality, ownership rights in data, data availability, and permissible clearinghouse use of data.

**Clearinghouse agreement.** A *clearinghouse agreement* can help to ensure sufficient certainty and reliability and a fair apportionment of liability

<sup>224</sup> Antitrust Div. Business Review Procedure, 28 C.F.R. § 50.6 (1990).

<sup>225</sup> Federal Trade Commission's Rules of Practice (CCH) pt. 1 subpt. A § 1.1 (1990).

between trading parties. It is recommended that a clearinghouse agreement be executed that addresses many of the relevant issues raised in this chapter.

### § 5.47 Clearinghouse Confidentiality Issues

Trading partner acceptance of the clearinghouse as a record holder or trusted intermediary requires that trading partner data be maintained in confidence by the clearinghouse. Certain clearinghouse activities are potentially subject to the Electronic Communications Privacy Act of 1986,<sup>226</sup> as well as applicable state privacy legislation, some of which is highly proscriptive.

Clearinghouse confidentiality issues likely will proliferate (1) as systems become more distributed, (2) as suppliers increasingly collect information about their customers (for example, *quick response* in the retail industry and just-in-time in manufacturing industries require significant and expedient data collection), and (3) as EDI is used to communicate increasingly personal or proprietary trade secret data. For example, there has been an increasing use of "people information," such as specialized data structures developed in the insurance and mortgage banking industries.<sup>227</sup> Privacy concerns have already contributed to the failure of a proposed clearinghouse.<sup>228</sup>

### § 5.48 —Clearinghouse Agency Status

When the clearinghouse mediates a communication between two trading partners, agency issues may arise. For instance, a trading partner seeking to repudiate an electronic contract may claim misfeasance by the clearinghouse.

Evaluation of the legal requirements of agency relating to the telegraph is instructive in considering the factors affecting clearinghouse responsibilities. Agency issues arose as a consequence of the development of the telegraph in the early nineteenth century. Arthur Corbin, a noted commentator on contract law, considered the situation in which a telegraph company introduced error into the transmission by slightly changing the price of the goods. He noted the conflicting case law on this point and decided

<sup>226</sup> Pub. L. No. 99-508, 18 U.S.C.A. § 2510 (West Supp. 1990).

<sup>227</sup> See letter from Donald H. Spiegel to Harriet Rusk (Dec. 20, 1989) (discussing Person-Oriented Transaction Sets, ASC X12S/89-742).

<sup>228</sup> See § 5.11.

not to subscribe to the policy of choosing one of the "innocent sufferers" to bear the entire loss:

Again, it may be said that the sender of the telegram has chosen the telegraph company as his agent, thus making it appear that some general rule of agency can be deductively applied. While it is true that the sender of a telegram knows that it must be translated by the clerks into a telegraphic code and back into words, with some possibility of error in the process, this is hardly enough to establish a relation of agency. Assuredly, the sender does not hold out the telegraph clerk as his agent with power to contract on his behalf. Nor is the clerk his servant. The telegraph company is a public servant, much like the post office . . . under compulsion to serve all comers and to bear the responsibility that accompanies public service.<sup>229</sup>

Similar questions, which on occasion lead to specific agreements, are now being raised with respect to the relationship between TPSPs and their users.<sup>230</sup> Although the contractual rules of TPSPs and clearinghouses generally expressly disclaim the existence of an agency relationship,<sup>231</sup> where the clearinghouse is intimately involved with electronic contract formation it may potentially be considered an agent of the user. Therefore, it is critical that the clearinghouse and its users reach agreement on all relevant agency issues.

### § 5.49 Clearinghouse Forecast

Clearinghouses represent important mechanisms to support reliable electronic trade. There is increasing demand for, and a movement toward, the provision of clearinghouse-like services in both the private and public

<sup>229</sup> A. Corbin, *Corbin on Contracts* Vol. I § 105 (1963).

<sup>230</sup> See *Butler v. Foley*, 211 Mich. 668, 179 N.W. 34 (1920) (court considered contract based on three telegrams in which defendant contended that telegraph company was plaintiff's agent for purposes of risk of error in transmission of defendant's reply); Whitter, *Restatement of Contracts and Mutual Assent*, 17 Calif. L. Rev. 441, 447-448 (1929); A. Corbin 1 *Corbin on Contracts* § 105 (1963); *Western Union Tel. Co. v. Cowin & Co.*, 20 F.2d 103 (8th Cir. 1927) (telegraph company is independent contractor responsible to both sender and receiver for errors); 10 *Williston* § 1134 (1967).

<sup>231</sup> For example, *CapitaLink* electronic bond auction trade rules expressly provide that it does not act as a principal in its transactions. *CapitaLink Bond Auctions, Inc.*, Rules of Participation (Mar. 1989). See also, § 12A Sample Agreement Originating Depository Financial Institution (ODFI)-Originator (Corporate) Agreement (Credit Entries), U.C.C. art. 4A; *Automated Clearinghouse System*, NACHA, at 62 (provides that automated clearinghouse is not an agent of ODFI).

sectors.<sup>232</sup> Private enterprise, trade associations, and the government are beginning to recognize the potential benefits to EDI of clearinghouses. Currently on-line database systems, real-time global securities trading and auctioning, and various intermodal transportation databases utilize clearinghouses. However, most clearinghouses are either limited in scope or in preliminary phases of development or implementation.

Some TPSPs have either contemplated the provision of or are currently providing, clearinghouse-like services, yet their ultimate success is questionable without (1) industry and standards-making-body involvement, (2) the resolution of attendant legal and control issues, (3) economic demand, and (4) support by mainstream business. The next few years surely will bring the clearinghouse to the forefront of electronic trade, with promise of contributing to the expansion and facilitation of electronic trade.

<sup>232</sup> See § 5.3. An EDI clearinghouse was proposed in 1988 within the CCITT X.400 standards community (recommendation X.400-430, Data Communications Networks: Message Handling Systems) as a "specialist 'EDI' VAN." See Contribution by G.E. Information Services to the CCITT X.400/EDI Interregnum Meeting (San Francisco Nov. 1988). This contribution proposed that service elements be provided for intermediary clearinghouse addressing.

A comparatively robust generalized EDI Clearinghouse was proposed in 1988 to be undertaken by the Data Interchange Standards Association Committee and industry associations. Baum, Fidelman, & Gerus, *EDI Clearinghouse Proposal* (1989).

TeleTrusT, an international organization composed of national TeleTrusT bodies, has been an important advocate of secure electronic commerce, including digital signature, legal recognition, and the general development of an infrastructure for public key cryptosystems and clearinghouse-like structures. National TeleTrusT bodies include those in Germany, Italy, the Netherlands, Sweden, Finland, and France, and they are under consideration in other nations.



## **APPENDIX C - "THE AUTOMATION OF THE NOTARY PUBLIC"**

*The Automation of the Notary Public begins on the next page.*

Excerpted from: Electronic Contracting, Publishing, and EDI Law, Michael S. Baum and Henry H. Perritt, Jr., ©1991, Wiley Law Publications. Reprinted by permission of John Wiley & Sons, Inc.





# **ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW**

---

**MICHAEL S. BAUM**

Member of the Bar  
of the State  
of Massachusetts

**HENRY H. PERRITT, JR.**

Professor of Law  
Villanova University  
School of Law



**Wiley Law Publications**

**JOHN WILEY & SONS, INC.**

**New York • Chichester • Brisbane • Toronto • Singapore**





### § 4.33 Notary Public

The notary public (notary) historically has played a role in ensuring the reliability of documents. However, the notary's potential role in ensuring the reliability of electronic transactions and records has not received formal legal scrutiny, despite changing business needs and practices.<sup>233</sup> Notarial automation includes support for computer-based mechanisms and procedures to authenticate electronically created, processed, communicated, and stored information and to provide related services<sup>234</sup> for legal purposes.

A *notary* is defined as

a public officer whose function it is to administer oaths; to attest and certify, by his hand and official seal, certain classes of documents, in order to give them credit and authenticity in foreign jurisdictions; to take acknowledgments of deeds and other conveyances; and certify the same; and to perform certain official acts, chiefly in commercial matters, such as the protesting of notes and bills, [and] the noting of foreign drafts . . . .<sup>235</sup>

An acknowledgment is a key notarial act intended to ensure the reliability of records. The concept of a notarial acknowledgment is further defined in the case law: "[A]n *acknowledgment* is the formal statement of the grantor to the official authorized to take the acknowledgment that the execution of the instrument was his free act and deed." It establishes the "identity of [the] person [acknowledging] and [the] genuineness of the signature attached to the instrument." A notary takes "the acknowledgment or proof of . . . instruments in writing executed by any person, and [gives] a certificate of such proof or acknowledgment, endorsed on or attached to the instrument . . . [and] signed by the notary."

A notary generally prints a *certificate of acknowledgment* on to a document that "establishes, at least *prima facie*, that the document to which it

was affixed was duly executed."<sup>236</sup> An acknowledged document is more readily accepted as authentic. The required acknowledgment procedures and recitals are specific to each state. Generally, procedures require physical presence of the signer, verification of identity, and signature.

Procedures and conventions exist to bolster the extraterritorial effect of notarial acts. Statutes in many states require authentication of the notary's signature, qualifications, and authority for documents acknowledged outside the state. Also, the form of acknowledgment often must conform to local law.<sup>237</sup> A *certificate of authenticity*, issued by an authorized official of the jurisdiction in which the acknowledgment was taken, such as the secretary of state, should be attached to the notary's certificate of acknowledgment.<sup>238</sup>

Certificates of authenticity are used both domestically, between states, and internationally. "A public notary is considered, not merely an officer of the country where he is admitted or appointed, but as a kind of international officer, whose official acts, performed in the state for which he is appointed, are recognized as authoritative the world over."<sup>239</sup> For instance, in ruling that a Norwegian notary's certificate of protest of a bill of exchange was properly received into evidence, an American court stated that "[t]he court will take judicial notice of the seals of notaries public, for they are officers recognized by the commercial law of the world."<sup>240</sup>

Where a notarization is performed by an officer of another country, the certificate of authentication must generally be under the great seal of that country. "An 'authentication' is a governmental rather than a notarial act by which a chain of authorities certify to the genuineness of the signature and seal and the position of a foreign official who has executed, issued, or certified a copy of a document so that the document executed or issued in one jurisdiction will be recognized in another."

The requirements for a certificate of authentication have been modernized by convention. The Hague Convention Abolishing the Requirement of Legalization of Foreign Public Documents<sup>241</sup> (Hague Convention) applies "to public documents [including notarial acts] which have been executed in the territory of one contracting State and which have to be produced in the territory of another contracting State."<sup>242</sup> The Hague Convention eliminates

<sup>233</sup> That is, with respect to providing electronic notarization services for electronic transactions and records notarization, which would thereby endow such acts with the legal standing afforded by conventional notarial acts.

<sup>234</sup> For example, a nonrepudiation service in an electronic environment "implies the existence of an agreed trusted third party . . . who may record the proof or generate the proof in real time." *Introduction to ISO/IEC JTC1/SC21/Proj. 97.21.9 Q53* (Nov. 1989).

<sup>235</sup> Black's Law Dictionary 956 (5th ed. 1979). The Uniform Law on Notarial Acts enumerates the following notarial acts: (1) taking an acknowledgment, (2) taking a verification, (3) witnessing or attesting a signature, (4) certifying or attesting a copy of a document, and (5) making or noting a protest. Unif. Law on Notarial Acts § 2, 14 U.L.A. 1 (1990 Supp.) [hereinafter ULNA].

<sup>236</sup> *Proof of Facts* 12 Am. Jur. § 3 (Acknowledgments), at 284 (1963); *Transamerica Title Ins. Co. v. Green*, 11 Cal. App. 3d 693, 89 Cal. Rptr. 915 (1970); ULNA, § 3(c). The certificate must be filled out in the presence of the person taking the acknowledgment. It may be criminal not to do so. *Citizens Nat'l Bank in Zanesville v. Denison*, 165 Ohio St. 89, 133 N.E.2d 329, 333 (1956).

<sup>237</sup> E.g., Mass. Gen. L. ch. 183, § 30 (1958).

<sup>238</sup> See, e.g., Eugene E. Hines, *A Manual for Notaries Public of Massachusetts* 4, 23 (American Society of Notaries 1977) [hereinafter Hines].

<sup>239</sup> *Wood v. St. Paul City Ry.*, 42 Minn. 411, 44 N.W. 308 (1890).

<sup>240</sup> *Pierce v. Indseth*, 106 U.S. 546, 549 (1883). See also *California v. Hollander*, 163 Cal. App. 2d 379, 329 P.2d 740 (1958) (California courts to take judicial notice of out-of-state notaries' seals).

<sup>241</sup> *Done at The Hague* Oct. 5, 1961. *Entered into force for the United States* Oct. 15, 1981 [hereinafter Hague Convention]. The Hague Convention has been endorsed by the ABA and the Dep't of Justice. A.B.A. House of Delegates Proceedings of 1983 Midyear Meeting at 398; A.B.A. House of Delegates Proceedings of 1975 Midyear Meeting at 243.

<sup>242</sup> Hague Convention, art. 1.

the requirements of proving a *chain of authentication* with the final diplomatic signature among member states.<sup>243</sup> "[T]he only formality that may be required in order to certify the authenticity of the signature, [and] the capacity in which the person signing the document has acted . . . is the addition of the [Apostille] certificate."<sup>244</sup> The Apostille takes the form represented in Figure 4-3.

<b>APOSTILLE</b> (Convention de La Haye du 5 Octobre 1961)	
1. Country.....	
2. has been signed by.....	
3. acting in the capacity of.....	
4. bears the seal/stamp of.....	
<b>Certified</b>	
5. at.....	6. the.....
7. by.....	
8. N°.....	
9. Seal/stamp:	10. Signature:

Figure 4-3. Form for Apostille certificate.

<sup>243</sup> It eliminates the "time-consuming and burdensome process . . . [of the] chain-certificate method of document certification." Letter of submittal from Joseph John Sisco, acting secretary of state, to the president (Apr. 8, 1976) (concerning the Hague Convention).

<sup>244</sup> Hague Convention, art. 4.

Simplification of the notarial process is evidenced nationally by the Uniform Law on Notarial Acts (ULNA), which dispenses with interstate certificates of authentication. The ULNA provides that:

- (a) A notarial act has the same effect under the law of this State as if performed by a notarial officer of this State if performed within the jurisdiction of and under authority of a foreign nation or its constituent units or a multi-national or international organization by any of the following persons: (1) a notary public or notary;
- (b) An "Apostille" in the form prescribed by the Hague Convention of October 5, 1961, conclusively establishes that the signature of the notarial officer is genuine and that the officer holds the indicated office.

### § 4.34 —Problems with Notarial Process

The office of the notary public has reached a critical juncture. Problems and criticisms of the notarial process make a compelling case for considerable reform. Weaknesses in the notarial system directly relate to the legal issues that create barriers to notarial automation and bolster the arguments for automation. The following weaknesses in the conventional notarial process have been identified:

**Evidentiary problems.** "[E]videntiary problems in establishing or disproving that there is a latent defect in a certificate or acknowledgment [are] . . . made more complex by the interrelation of questions as to the dignity to be accorded the certificate, the weight to be accorded recitals of fact contained in it, matters of public policy, the recording of laws, presumptions, possible estoppel, and the competency of witnesses."<sup>245</sup>

**Incompetence.** A recent study of notaries in New York revealed that "of a group of 217 notaries, only one completed the notarial procedure correctly. The study further indicated that of the notaries questioned: 97.7% were unfamiliar with the authentication procedure that verifies certificates issued by notaries; and 88.6% neglected to administer the required oath to the affiant; and 82.5% failed to check the affiant's identification."<sup>246</sup> These findings have prompted some states to initiate notarial reform efforts: "[I]n

<sup>245</sup> 12 Am. Jur. *Proof of Facts* § 4, at 284, 285.

<sup>246</sup> Home Sav. of Am. v. Einhorn, No. 87 C 7390, 190 WESTLAW 114643 (N.D. Ill. July 24, 1990). A representative from one notary association suggests that statistical bias in the New York study overstates the extent of notarial incompetence and that probably only 10% of notaries may have acted negligently. Telephone interview with Charles Faerber, vice-president of legislative affairs, National Notary Association, Canoga Park, Cal. (Sept. 3, 1990).



light of these results (which do not contradict common experience), it may be questioned whether notarization is actually an improvement upon the mere signature of the declarant."<sup>247</sup>

**Insufficient identification.** According to one source, "[o]ne of the most common complaints of negligence against notaries involves their alleged failure to identify the person seeking the acknowledgments."<sup>248</sup>

**Lack of personal presence and oath.** "It is a matter of common knowledge that, in many instances, notaries acknowledge signatures to claims, affidavits, depositions, and verifications without the signer actually being present; and also that quite often, when the signer is present, nothing is said about an oath and no thought is given to it whatever, thus raising a serious doubt as to whether a solemn oath had actually been administered by the notary and taken by the signer."<sup>249</sup>

These notarial deficiencies, as well as practical concerns such as economy, have prompted a "national trend toward a liberal rather than technical interpretation of notary acknowledgments,"<sup>250</sup> which is evidenced by statutory and case law reforms. The reforms have increased use of self-sworn documents.<sup>251</sup>

<sup>247</sup> *Home Sav. of Am. v. Einhorn*. Some states, including Florida, have begun to revise the notarial process. The general counsel of the Florida Dep't of State explained that "[w]e want to make the notarial process mean something—or do away with it altogether." *Id.* Considerable notarial incompetence raises new concerns about notarial automation given the likely requirement for familiarity and proper use of computer technologies.

<sup>248</sup> Annotation, *Notary Public or Bond-Liability* 44 A.L.R.3d 559 (1972).

<sup>249</sup> *State v. Heyes*, 44 Wash. 2d 579, 269 P.2d 577, 582 (1954). Generally, the purpose of the oath is to impress upon its taker the importance of providing accurate information. See *People v. Ramos*, 430 Mich. 544, 548, 424 N.W.2d 509, 511 (1988) ("An oath signifies the undertaking of an obligation 'to speak the truth'."); *State v. Grant*, 176 Conn. 17, 404 A.2d 873, 877 (1978).

<sup>250</sup> Larroumet, *Detrimental Reliance and Promissory Estoppel as the Cause of Contracts in Louisiana and Comparative Law*, 60 Tulane L. Rev. 1209 (June 1986) (technical deficiency of a jurat).

<sup>251</sup> For example, a federal statute provides that:

[W]herever, under any law of the United States or under any rule, regulation, order, or requirement made pursuant to law, any matter is required or permitted to be supported, evidenced, established, or proved by the sworn declaration, verification, certificate, statement, oath, or affidavit, in writing of the person making the same (other than a deposition, or an oath of office, or oath required to be taken before a specified official *other than a notary public*), such matter may, with like force and effect, be supported, evidenced, established, or proved by the unsworn declaration, certificate, verification, or statement, in writing or such

The following is a sampling of these reforms:

1. The implementation of alternative acknowledgment procedures laws increasingly provides for non-notarially administered oaths.
2. The choice of notarization or declaration by the signatory is now being provided by many federal circuit courts of appeal.<sup>252</sup>

person which is subscribed by him, as true under penalty of perjury, and dated, in substantially the following form:

(1) If executed outside of the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date).

(2) If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date).

(Signature)

28 U.S.C.A. § 1746 (West Supp. 1976) (emphasis added). Various states are considering revising their notarial laws to conform with this federal statute, for example, Kansas: "AN ACT concerning certain unsworn declarations; permitting such declarations under penalty of perjury in certain instances; amending K.S.A. 1984 Supp. 21-3805 and repealing the existing section." H.R. 2453 \_\_\_\_\_ (1985) and H.R. Bill 2082 \_\_\_\_\_ (1987). 18 U.S.C. § 1001 (1988) states: "The undersigned being hereby warned that willful false statements and the like so made are punishable by fine or imprisonment, or both, and that such willful false statements may jeopardize the validity of the application or any resulting registration [cited in application for trademark]."

The legislative history to this law provides insight into its purpose and operation:

The purpose of this legislation is to permit the use in Federal proceedings of unsworn declarations given under penalty of perjury in lieu of affidavits. . . . The requirement that the person who signs an affidavit must appear before a notary and be sworn can be inconvenient. For example, it may be necessary for the document to be executed during other than normal business hours. Further, the document may have to be executed in another country for use in the United States. This generally will require, in addition to the document subscribed to under oath, additional certifications and documents to prove such things as the authenticity of the officer who administers the oath and the authenticity of his seal.

The legislation provides an alternative to affidavits and sworn documents when it is necessary to require verification of the truthfulness of what the document contains. The legislation will permit the signer to subscribe to a document that expressly provides that it is being executed subject to the penalties of perjury—a procedure already in use with the federal income tax return form 1040.

26 U.S.C. §§ 6065, 7206(1) (1988). Consistent with this law, IRS Regulations provide that "a power of attorney must be acknowledged before a notary public, or in lieu thereof, witnessed by two disinterested individuals." 26 C.F.R. § 601.504 (1990).

<sup>252</sup> On the state level, California has for 19 years permitted the use of unsworn declarations given subject to the penalty of perjury. The experience under the California statutes has been positive, and the State Bar of California has endorsed the purpose of the legislation.

To address the concern that a prisoner may wish to file a complaint but does not have access to a notary, circuit courts may offer prospective complainants an alternative of

3. The requirement that transfers of automobile title be notarized is being eliminated by Florida, Missouri, and Texas, among other states.
4. The short form granting power of attorney in New York no longer requires notarization.
5. New York has modified its penal law to provide for "verification by means of a form notice . . . which is the procedural equivalent of the more traditional type of oath or affirmation. . . . This provision 'was specifically enacted by the Legislature in order to provide a convenient method of assuring the truthfulness of documents without resort to the often cumbersome procedure of requiring an oath before a notary.'"<sup>253</sup>

### § 4.35 —Automation of Notarial Process

Given the recognized deficiencies of current notarial practices and the ongoing liberalization trend, plus increased use of data communications technologies, it is time to consider automation of notarial functions. Automation could effectively improve current business practices and provide greater reliability for electronic transactions and records.

Automation of the notarial process can accommodate modern business practices by improving the reliability, economy, and speed of electronic transactions and records.<sup>254</sup> The following notarial services could support electronic trade transactions. Each would entail the use of increasingly sophisticated technologies and would liberalize notarial requirements.

**Notarization of agreements for electronic trade.** The notary could attest to the parties' assent by means of conventional, paper-based agreements, such as trading partner or interchange agreements, to conduct electronic trade, as well as to the underlying terms and conditions. Such notarization is intended to authenticate the intention of the parties subsequently to bind themselves electronically. In this role, the notary provides *only* conventional, paper-based, notarial services in support of electronic trade.<sup>255</sup>

submitting to either an oath or a declaration. Federal Judicial Center, *Illustrative Rules Governing Complaints of Judicial Misconduct and Disability with Commentary*, Rule 2(f) (1981).

<sup>253</sup> *People v. Webster*, 161 A.D.2d 960, 557 N.Y.S.2d 533, 534 (1990) (quoting *People v. Sullivan*, 56 N.Y.2d 378, 383, 437 N.E.2d 1130, 452 N.Y.S.2d 373 (1982)). The New York form notice provision is contained in N.Y. Penal Law § 210.45.

<sup>254</sup> Or, at a minimum, can provide insight into issues and requirements for digital notarization.

<sup>255</sup> Where such notarized agreements are retained in electronic form and are electronically accessible to other trading partners, the notary arguably plays a hybrid conventional/

**Notarization of electronic media.** Notarization in electronic media may include:

1. Attesting to the accuracy of an electronic record (as sent or received) or a printout of an electronic record. Notaries have the power to make certified copies of instruments on file and thereby authenticate them.<sup>256</sup>
2. Acknowledging the sealing of a data tape or other physical media. The attestation of data contents and of sealing a data tape are akin to a notary's conventional duties of listing and sealing property contained in a bank vault or safe-deposit box.<sup>257</sup>
3. Attesting to the contents of electronic records. This could include attestation to the integrity of all file names or to the data content of a particular data tape (used to electronically store data in a physical envelope or other tamper-resistant enclosure) or to the absence of such information from a data tape.<sup>258</sup>

**Attesting to computer-based acts.** This might include attesting to having observed a person physically enter certain information into a computer or to having observed a person "sign" a computer document either by entering

electronified role. See Baum, *Contract Facilitating Services*, EDI and the Law § 9.11 (I. Walden ed. 1989).

<sup>256</sup> E.g., N.Y. Civil Practice Act §§ 329, 330, 367, 368, 373, and 374 [superseded by the N.Y. Civ. Prac. L. & R.]. With respect to copies, a notary may attest: "[t]hat I have compared the annexed copy letter with the original thereof exhibited to me by [name of person, address, date] together with the envelope duly postmarked and addressed to [name and address of recipient] purporting to have contained said letter and that the same is a true copy thereof and of each and every part and the whole thereof." Blaustein at 60. The electronic authentication of hardcopy versions of data is currently a contentious topic in the electronic messaging and security technical communities because of significant technical problems of verifying electronically created paper documents.

<sup>257</sup> See, e.g., Mass. Gen. L. ch. 167 § 32 (1984).

<sup>258</sup> Cf. *United States v. Farris*, 517 F.2d 226 (7th Cir.), cert. denied, 423 U.S. 892 (1975) (officially certified computer data compilations were self-authenticating and properly admitted into evidence, for purpose of showing income tax returns had not been filed). A notary could observe the data content on a computer's VDT or in a printout.

The P<sub>edi</sub> standard (see § 4.24) refers to a "notarizing function" and indicates that notary use is possible within its framework. CCITT X.435, cl. 17.1.2. However, little work has been done to explicitly describe the use of notaries. Notarization is defined in the ISO Security Architecture as "[t]he registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery." ISO 7498-2-1988(E), §§ 3.3.37, 5.3.8. ANSI standards describe notarization as "a method of applying additional security to a key utilizing the identities of the originator and the ultimate recipient (ANSI X9.17), cited in ANSI X12.58 (Security Structures) at 11.



his or her name, symbol, or code or by undertaking the necessary act(s) to electronically sign a computer-based document.<sup>259</sup>

**Authenticating security credentials.** This might include the authentication of the correlation (binding) between a user's security credentials, such as a public key certificate, and the user that it purports to authenticate.<sup>260</sup> An electronic chaining of authentication is important for cryptographic purposes, such as for the authentication of messages and security credentials using public key certificates, and it presents important parallels that are largely beyond the scope of this inquiry. Absent private agreement, electronic *cross-certification* between root issuers of security credentials bears similarities to *letters rogatory*, a judicial request of one court to a court in another jurisdiction to facilitate discovery.<sup>261</sup> Also, the use of *nested* signatures can provide even greater assurances of authenticity. The notary could review a document, use signature and public key material to verify correctness, and then attach his signature and public key material.

**Serving as a disinterested electronic record keeper or verifier.** A trusted entity, such as a clearinghouse, a government instrumentality,<sup>262</sup> or possibly a TPSP, could attest to the regularity of electronic record keeping. Messages that would benefit from assurances against repudiation could be sent to a notary, who would undertake a variety of proof-related services,

<sup>259</sup> *Ed.*, the author is cognizant of the potential weaknesses in such computer-based practices where the computers do not exist within a trusted (secure) environment. Establishing a baseline of required trust will be necessary. See § 4.19 on a security baseline.

The definition of notary functions in at least one state specifically authorizes notaries to certify the occurrence of an event. "Notarial act" and "notarization" mean . . . (g) certifying that an event has occurred or an act has been performed." Wash. Rev. Code § 42.44.010 (2) (1986).

<sup>260</sup> Security credentials may include issuer name, validity period, and cryptographic algorithms identifier.

<sup>261</sup> *In re Application of Dist. Attorney of Queens County*, 132 Misc. 2d 506, 505 N.Y.S.2d 293, 294 (N.Y. Sup. Ct. 1986). *Magdanz v. District Court of Woodbury County*, 222 Iowa 456, 269 N.W. 498, 499 (1936); *ECCO High Frequency Corp. v. Amtorg Trading Corp.*, 276 A.D.2d 827, 93 N.Y.S.2d 178 (1949). The granting of letters rogatory rests entirely upon the international comity of courts. See *Lastram Corp. v. Hale*, 438 So. 2d 269, 271 (La. Ct. App. 1983). See Fed. R. Civ. P. 28(b) (letters rogatory for depositions).

<sup>262</sup> Various government models for record keeping exist, such as the statutory requirement for publishers, known as *legal deposit*, to deliver all new publications to a national library (see 17 U.S.C. § 408(b) (1982)) and *copyright deposit* under the federal copyright law. See Crews, *Legal Deposit in Four Countries: Laws and Library Services*, 80 L. Library J. 551 (1988). The role of the notary as a record keeper is firmly established in many countries, such as France and China. Tung-Pi Chen, *The Chinese Notariat: An Overlooked Cornerstone of the Legal System of the Peoples Republic of China*, 35 Int'l & Comp. L.Q. 69, 70 (1986).

including overseeing the attachment of an accurate time and date stamp to a message, logging the time messages sent or received, attesting to the proper storage of electronic records, and comparing and certifying the authenticity or integrity of cryptographically enhanced messages.<sup>263</sup>

**Accommodating electronic notarization device.** This might include a secure (tamper-resistant) device certified by a disinterested third party, such as a notary, and used independently for electronic notarizations. Such a device can be characterized as an *electronic notary agent*.

### § 4.36 —Potential Legal Barriers to Notarial Automation

The law may not sufficiently accommodate notarial automation. For example, narrow or conservative construction of definitions (such as for a *writing* or *signature*) and conventional notarial practices may impede automation. It has been said that notarial acts "ought to give evidence touching such things as fall under [a notary's] corporeal senses."<sup>264</sup> Because information in electronic form is less corporeal or physical, it presents a challenge to traditional notarial practices. Obviously, automation of the notarial process could not have been contemplated in prior centuries. However, even current law does not expressly accommodate the electronic notary and in certain circumstances it may actually impede such practices.<sup>265</sup> This section considers notarial requirements that constitute potential legal barriers to automation and the methods that may be used to overcome such barriers.

<sup>263</sup> Mechanisms or products that are targeted to provide notary-like services include BITPROOF, The Electronic Notary Public, by the Public Signature Company, which applies a 64K digital signature using the El Gamal algorithm, a method to time-stamp digital documents. *Cf.* mechanism for time-stamping digital documents that eliminates the requirement of an intermediary by linking "bits from the previous sequence of client requests in the signed certificate." Haber and Stornetta, *How to Time-Stamp a Digital Document*, paper presented to CRYPTO '90, at 4 (1990).

<sup>264</sup> Hines (citing John Ayliffe, *Parergon Juris Canonica Angeligani* 302 (London, 1726)).

<sup>265</sup> Electronic notarization mechanisms have been described as those:

trusted by the communicating entities, and which hold the necessary information to provide the required assurance [of integrity, origin, time, and destination] in a testifiable manner. Each instance of communication may use digital signature, encipherment, and integrity mechanisms as appropriate to the service being provided by the notary. When such a notarization scheme is invoked, the data is communicated between the communicating entities via the protected instances of communication and the notary.

ISO 7498-2-1988(E) § 5.3.8.1.

### Physical Presence

Notarial laws generally require persons making affidavits or acknowledgments to do so "before" or "in the presence of" a notary public.<sup>266</sup> In certifying an acknowledgment, a notary must either have personal knowledge of the individual who makes it or be satisfied as to his or her identity by taking various precautionary steps.<sup>267</sup> This requirement is intended to prevent fraud by precluding mistaken identification, disability, and duress. Notarization in the absence of the affiant's physical presence is limited to certain predefined notarial acts.<sup>268</sup>

It is a dubious assumption that physical presence improves the authenticity of a conventionally notarized document. Evidence suggests that as a practical matter, physical presence before a notary does not necessarily serve its intended purpose of preventing fraud. For example, duress or overreaching are not necessarily evident to a notary where the affiant is threatened with blackmail or future physical violence. Similarly, the influence of drugs is not necessarily detectable by a notary. Consequently, the making of an acknowledgment under these circumstances does not prove that it was undertaken freely and voluntarily.

Where the notary relies on the presentation of information to prove an affiant's identity, forged identification documents and the failure to scrutinize the documents adequately may vitiate their effectiveness. Finally, certificates of authenticity generally are procured without requiring the physical presence of the attesting notary.

In order to accommodate electronic practices, notarial conventions of questionable value, such as the requirement of physical presence, must be relaxed. The benefits of electronic transactions are premised on their speed and efficiency. Physically traveling to a notary and undertaking conventional notarial ceremonies within an electronic environment is impractical. Such an undertaking would eliminate or severely reduce the speed and low-cost benefits of electronic data interchange. Thus, it is imperative to facilitate mechanisms that establish the legal sufficiency of remote or long-distance notarial acts that occur outside the notary's personal presence.

<sup>266</sup> *De Camp v. Allen*, 156 So. 2d 661, 663 (Fla. Dist. Ct. App. 1963) (officer held liable for damages by notarizing and taking an acknowledgement of signatories who had not personally appeared before the notary). The *comment* to ULNA § 2 provides that "personal physical appearance of the acknowledging party before the notarial officer is required."

<sup>267</sup> *Ardis v. State*, 380 So. 2d 301, 304 (Ala. Crim. App. 1979).

<sup>268</sup> The nature of the permitted notarial acts is limited in accordance with their perceived seriousness. For example, the making of a criminal complaint before a notary public is insufficient. Instead, the presence of a government official is required to ensure reliability and fairness. *See Locke v. Burns*, 160 W. Va. 753, 238 S.E.2d 536, 538 (1977).

Electronic technology can provide integrity comparable to—or, more often, greater than—that attainable through some conventional notarial practices. Cryptography can provide high assurances of authenticity and integrity, and various devices can control access, as well as assess physical disability (such as intoxication).<sup>269</sup> More extensive liberalization of the requirements regarding a notary's physical presence are to be expected.<sup>270</sup>

### Proof of Identity

According to the Uniform Law on Notarial Acts (ULNA), "[A] notarial officer has satisfactory evidence that a person is the person whose true signature is on a document if that person . . . is identified on the basis of *identification documents*."<sup>271</sup> The ULNA enumerates the items sufficient to establish individual identity:

"[S]atisfactory evidence," as it pertains to identification on the basis of documents . . . means identification as an individual based on at least one current document issued by the federal or a state government with the individual's photograph, signature and physical description, or at least two documents issued by an institution, business entity or federal or state government with at least the individual's signature.<sup>272</sup>

<sup>269</sup> Some such technologies are not prevalent and might not be widely available in the near future. However, the user's personal presence will remain necessary to establish the initial correspondence (binding) between an individual and her/his electronic credentials (for example, public key certificate).

<sup>270</sup> Further reform may be undertaken for teleconferenced and videotaped depositions. Telephone interview with Charles N. Faerber, vice-president of legislative affairs, National Notary Association, Canoga Park, Cal. (Sept. 3, 1990).

<sup>271</sup> ULNA, § 2(f) (emphasis added).

<sup>272</sup> Or. Rev. Stat. § 194.505(8) (1989) (variation from the official text of ULNA, § 1). California's Notary Public Statute sanctions the use of specific documents to authenticate certain notarial acts:

If a notary public executes a jurat and the statement sworn or subscribed to is contained in a document purporting to identify the affiant, and includes the birthdate or age of the person and a purported photograph or finger or thumbprint of the person so swearing or subscribing, the notary public shall require, as a condition to executing the jurat, that the person verify the birthdate or age contained in the statement by showing either:

- (a) A certified copy of the person's birth certificate, or
- (b) An identification card or driver's license issued by the Department of Motor Vehicles.

CSN § 8230, Identification of Affiant; Verification. *See* Annotation, *Admissibility, in Action against Notary Public, of Evidence as to Usual Business Practice of Notary Public of Identifying Person Seeking Certificate of Acknowledgement*, 59 A.L.R. 3d 1327 (1974) (discusses the admissibility of evidence concerning the notary public's standard business practice of identifying a person seeking a certificate of acknowledgement).



It has been held sufficient proof of identity that a person was introduced to a notary by someone known and trusted by the notary despite the absence of documentary evidence.<sup>273</sup> As a reflection of modern urban society, notaries increasingly do not have personal knowledge of the affiant and are often not introduced by a person known and trusted by the notary.

Electronic technologies can provide high assurances of the authentic identity of an affiant. Additionally, electronic transactions can provide assurances of integrity through supplemental *out-of-band* mechanisms such as telephone communications. However, the use of out-of-band communications is inconsistent with the purpose of notarial automation.

### Oaths

Notaries are often required to administer an oath.<sup>274</sup> A recent case held that the use of a telephonically administered oath fulfilled the oath's underlying rationale:

An 'Oath or affirmation' is a formal assertion of, or attestation to, the truth of what has been, or is to be, said. It is designed to ensure that the truth will be told by insuring that the witness or affiant will be impressed with the solemnity and importance of his words. The theory is that those who have been impressed with the moral, religious or legal significance of formally undertaking to tell the truth are more likely to do so than those who have not made such an undertaking or been so impressed. We cannot accept . . . [the] argument that for constitutional purposes an oath or affirmation is invalid merely because it is taken over the telephone. *The moral religious and legal significance of the undertaking remains the same whether the oath taker and the witness communicate face-to-face or over the telephone.*

We hold that search warrant application procedures can constitutionally be brought into line with twentieth century technology.<sup>275</sup>

<sup>273</sup> *Immerman v. Ostertag*, 83 N.J. Super. 364, 199 A.2d 869 (1964).

<sup>274</sup> See ULNA § 1(3) ("Verification upon oath or affirmation" means a declaration that a statement is true made by a person upon oath or affirmation."). A Kansas court discussed the evidentiary effect of the notary's jurat: "[A] notary's certificate, or jurat, is presumptive evidence that the oath was administered, and so long as the jurat is unimpeached it is conclusive." *Fisher Lumber Co. v. Williams*, (1988 LW 2677 Kan. App.—Slip Copy). See *State v. Lewis*, 85 Wash. 2d 769, 539 P.2d 677 (1975) (irregularity in administering or taking of an oath is no defense to a prosecution for perjury under Wash. Rev. Code Ann. § 9.72.030 (1975)).

<sup>275</sup> *People v. Snyder*, 181 Mich. App. 768, 449 N.W.2d 703, 706 (1989) (use of telephone and fax machine to obtain warrant authority to withdraw sample of defendant's blood satisfied constitutional protections) (quoting *United States v. Turner*, 558 F.2d 46, 50 (2d Cir. 1977)) (emphasis added).

The law has begun to accommodate new technologies. For example, proof of acknowledgment by telephone<sup>276</sup> and telephone depositions<sup>277</sup> have been increasingly permitted; one state permits administering oaths in another state.<sup>278</sup> This liberalization should be extended to oaths communicated via reliable electronic data communications, for instance, an oath typed on a computer and reliably communicated electronically or an oath in the form of a referenced encoding within an EDI transaction.

### Writings and Signatures

In undertaking notarial acts, a notary is generally required to sign a certificate evidencing the notarial act.<sup>279</sup> The signature is generally *prima facie* evidence that the signature is genuine and that the person holds the title indicated.<sup>280</sup>

Increased automation of the notarization process will entail a reconsideration of the various attendant writing and signature issues, such as the time at which the notary's signature is applied, the acceptability of an electronic writing and signing, and the requirements that a writing and signing appear in prescribed forms. Each of these issues is considered in turn.

**Time of writing and signature.** A notarial acknowledgment "is a statement that the person has signed and executed an instrument; it is not the act of signature itself. Hence a person may appear before a notarial officer to acknowledge an instrument which that person had *previously* signed."<sup>281</sup>

**Electronic writing and signature sufficiency.** Although writings and signatures typically are not defined by notarial statutes, such definitions (as well as the accompanying issues and problems) are likely comparable to those assigned to writings and signatures under a statute of frauds.<sup>282</sup> If a

<sup>276</sup> See generally annotation, 3 *Proof of Facts, Conversations, Proof No. 2 (Acknowledgment by Telephone)*, 12 A.L.R. 538, 58 A.L.R. 604.

<sup>277</sup> Fed. R. Civ. P. 30(b)(4). See *Manual for Complex Litigation* 41.38(10) (1985). Legislation introduced in the Virginia legislature would allow notaries, "by agreement of the parties, [to] . . . administer an oath for the deposition of a witness whether or not the witness is physically present before the notary." (S. 124, "A bill to amend and reenact § 47.1-12 of the Code of Virginia, relating to powers of notaries." Offered Jan. 16, 1990).

<sup>278</sup> Alaska Stat. § 21.06.170 (1984). ULNA initially contained a provision that would have permitted telephone oaths. This provision was subsequently omitted.

<sup>279</sup> E.g., Or. Rev. Stat. § 194.565 (1989).

<sup>280</sup> ULNA §§ 3(c), 4(c), 5(b).

<sup>281</sup> *Comment* to ULNA § 2 (emphasis added).

<sup>282</sup> For example, U.C.C. § 1-201(39) (1989) defines a signature as "any symbol executed or adopted by a party with present intention to *authenticate* a writing" (emphasis added).

notarial statute does not proscribe electronic signatures, the acceptability of electronic "writings and signatures" should not be viewed as unequivocally foreclosed. Digital signatures should be considered binding to the same extent as conventional signatures.<sup>283</sup>

### Seals

A notarial seal or stamp is a tool intended to authenticate certain notarial acts. The notarial seal is generally prima facie evidence that the signature is genuine and that the notary holds the indicated title.<sup>284</sup> Seals vary along four dimensions: mode of impression, shape and size, content, and jurisdiction.<sup>285</sup> The notarial acts that require the use of a notarial seal vary by state,<sup>286</sup> and the significance of such seals is in decline.<sup>287</sup> Handwritten signatures have increasingly been recognized as a substitute for the notarial seal if, for instance, "L.S. locus sigilli" (place of seal) appears and is satisfied by a written signature.

Conventional notarial seals are fraught with weaknesses. They are available by mail order in many states without any requirement of proof of commission or vendor verification that an individual is authorized to use

U.C.C. § 5-104(2) (1989) provides that "a telegram may be a sufficient signed writing if it identifies its sender by an authorized authentication. The authentication may be in code or the authorized naming of the issuer in an advice of credit is a sufficient signing" (emphasis added). See *An Examination of U.C.C. Article 5 (Letters of Credit)*, 45 Bus. Law. 1645 (1990); See also *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement*, 45 Bus. Law. 1645 (1990).

<sup>283</sup> Most U.C.C. cases have focused on the *intention* of the parties to authenticate a writing, rather than on the required strength of the authentication. However, because notarial statutes are designed to provide for the authentication of documents, the stringency of the authentication required may be greater than that required under other laws. For a consideration of signatures and their relationship to authentication and security issues, see generally EDI Committee, *Proposed American Bar Association Policy Recognizing Security Techniques in Electronic Transactions*, 1991 A.B.A. Sec. Sci. & Tech.

<sup>284</sup> ULNA § 6(d).

<sup>285</sup> Vastrick, *The Examination of Notary Seals*, 27 J. Forensic Sci. 899, 901 (1982) [hereinafter Vastrick]. For discussion of computer-based examination of seals to discover fraud, see Tang, *A Computer-Aided Seal Discriminating System*, 33 J. Forensic Sci. 969 (1988).

<sup>286</sup> For a comprehensive treatment of state notarial seal requirements, see Vastrick at 906-10.

<sup>287</sup> See Hoath, *The Sealing of Documents—Fact or Fiction*, 43 Mod. L. Rev. 415 (July 1980) [hereinafter Hoath] ("[G]rantor's signature has assumed greater practical significance than the seal in showing the authenticity of a deed."). Fed. R. Evid. 902 (self-authentication) provides that "[e]xtrinsic evidence of authority as a condition precedent to admissibility is not required with respect to . . . (2) Domestic public documents not under seal . . . [and] (3) Foreign public documents."

such seals. Such access renders notarial seals available for illegitimate purposes.<sup>288</sup>

**Technological change in seals recognized.** Technological advances in the form and use of seals has historically been accommodated. For example, the Supreme Court has sanctioned the change from seals embossed by wax to seals imprinted on paper.<sup>289</sup> "The use of wax, or some other adhesive substance upon which the seal of a public officer may be impressed, has long since ceased to be regarded as important."<sup>290</sup> At common law, notaries may provide seals of their own choice.<sup>291</sup> The Uniform Commercial Code (UCC) has eliminated the requirement that sealed instruments be used in sales transactions.<sup>292</sup>

**Electronic seals sanctioned.** An electronic seal, such as a digital signature, can provide greater assurance of authenticity and is less forgeable than a conventional seal. In addition, such a seal can prove sufficiently permanent. The flexibility provided by most state statutes concerning the use of seals and the trend, noted above, toward the liberalization of their use are consistent with, and may provide a foundation for, legal acceptance of the "electronic seal," i.e., the digital signature when applied by a notary public.

**Placement of the electronic seal.** The seal need not be placed in any particular location on the certificate of authenticity.<sup>293</sup> Electronic seals can either be placed on or attached to the document. When the sequence of the seal's application is a legal requirement, electronic notarization can guarantee the accuracy of the application sequence.

<sup>288</sup> Vastrick at 903.

<sup>289</sup> Formerly wax was the most convenient, and the only material used to receive and retain the impression of a seal. . . . We cannot perceive why paper, if it have that capacity, would not as well be included in the category. The simple and powerful machine, now used to impress public seals, does not require any soft or adhesive substance to receive or retain their impression. The impression made by such a power on paper is as well defined, as durable, and less likely to be destroyed or defaced by vermin, accident, or intention than that made on wax. It is the seal which authenticates, and not the substance on which it is impressed; and where the court can recognize its identity, they should not be called upon to analyze the material which exhibits it.

Pillow v. Roberts, 54 U.S. (13 How.) 472, 473-74 (1851).

<sup>290</sup> Pierce v. Indseth, 106 U.S. 546, 548, 1 S. Ct. 418, 421 (1883).

<sup>291</sup> Kirksey v. Bates, 7 Port. 529, 31 Am. D. 722 (1838).

<sup>292</sup> "The affixing of a seal to a writing evidencing a contract for sale or an offer to buy or sell goods does not constitute the writing a sealed instrument and the law with respect to sealed instruments does not apply to such a contract or offer." U.C.C. § 2-203 (1989) (seals inoperative).

<sup>293</sup> Osgood v. Sutherland, 36 Minn. 243, 31 N.W. 211 (1886).



### Further Support for the Electronic Notary

**Presumption of regularity of notarial acts.** Each state's notarial powers can be classified as either *judicial* or *ministerial*. Judicial notarial acts carry the weight of a court judgment or are regarded as generally conclusive evidence.<sup>294</sup> When considered ministerial, notarial acts generally provide prima facie proof of the notarial act or rebuttable evidence of such act. Most states consider notarial acts ministerial.<sup>295</sup> Generally, courts are more likely to apply more lenient standards in reviewing the evidentiary effect of ministerial notarial acts. Such flexibility should additionally be extended to electronic notarization when it is deemed ministerial in nature.

**Substantial compliance.** Notarial statutes generally require notaries to sign certificates of acknowledgment and to provide other information, such as the date of the attestation and the date on which the notary's commission expires. However, the failure to include certain information, such as the notary's commission expiration date, will not invalidate the certificate.<sup>296</sup> "The absence of, or a defect in, the date of a certificate does not make it void;<sup>297</sup> nor does omission to state the place of the notary's residence, or failure to state the date of expiration of the notary's commission . . . unless statutorily required." Inclusion on the certificate of acknowledgment of the name of the county is not critical, although provision of the name of the state is. Many statutes require substantial but not literal compliance with forms of acknowledgment. For instance, a case held that "[t]echnical deficiencies in the certificate of acknowledgement may be cured by reference to the instrument itself."<sup>298</sup> Reliable automated notarial acts should, in this regard, be viewed as substantially in compliance with many notarial laws.

<sup>294</sup> See *State v. Heyes*, 44 Wash. 2d 579, 269 P.2d 577, 581 (1954) (in the case of judicial notarial powers, notarial acknowledgment can be attacked "only in the manner and for the causes of a judgment of a court of record").

<sup>295</sup> *Notaries*, 66 C.J.S. § 1.b. (1950) (citing *In re Butler*, 76 Neb. 267, 107 N.W. 572 (1906)).

<sup>296</sup> *Tildesley Coal Co. v. American Fuel Corp.*, 130 W. Va. 720, 45 S.E.2d 750 (1947); *Sheridan County v. McKinney*, 79 Neb. 223, 115 N.W. 548 (1908). The expiration date is considered directory rather than mandatory. ULNA, § 7(a) provides that the omission of the date of expiration on a notarial certificate of authentication "may subsequently be corrected." See also *Stern v. Board of Elections*, 14 Ohio St. 2d 175, 237 N.E.2d 313, 317-18 (1968) (omission of signature and seal).

<sup>297</sup> *Updegraff v. Palmer*, 107 Ind. 181, 6 N.E. 353 (1886) (statutory provisions concerning design and characteristics of seals have been held to be only directory, rather than prescriptive). *Sonfield v. Thompson*, 42 Ark. 46, 48 Am. Rep. 49 (1883).

<sup>298</sup> *Big River Grain, Inc. v. Small Business Admin.*, 718 F.2d 970 (9th Cir. 1983).

**De facto notary.** A de facto notary is "[g]enerally a person acting as a notary under color of authority with public acquiescence . . . and as to the public and third parties his acts are valid and cannot be attacked collaterally."<sup>299</sup> The electronic notary is not specifically sanctioned legislatively and therefore does not inherently possess commissioned notarial powers. However, when electronic notarial-like entities or systems are implemented by government instrumentalities for authentication and integrity purposes, query whether such an entity may hold de facto notarial powers.<sup>300</sup>

**Estoppel.** When the parties to an electronic transaction have contractually expressed their intention to recognize the validity of electronic notarial acts<sup>301</sup> or when the parties have repeatedly used electronic notarial services, estoppel may subsequently bar them from denying the validity of such acts. The express intentions of the parties to such transactions should overrule any competing public policy concerns raised by such estoppel.

**Improved record keeping.** Some states require a notary to keep a record of some or all of his or her official acts.<sup>302</sup> The extent to which such records are regularly and officially maintained may affect their admissibility into evidence as business records. Where applicable, notarial record-keeping requirements generally pertain to such information as the date of notarization; the name of the person executing the document; the name of the person/entity to which the document is intended to be sent; the fee (if any) for notarial services; the date of the document, whether the signatory's identity was based on personal knowledge or satisfactory evidence; and a description of the document notarized.<sup>303</sup> Electronic notarization can provide an automatic and complete record of notarial acts and thereby substantially improve notarial record keeping.

<sup>299</sup> *Notaries*, 66 C.J.S. § 5 (1950) (citing *Brown v. Anderson*, 210 Ark. 970, 198 S.W.2d 188, 191 (1946)) (also distinguishes *de jure* notaries). See *Mayer v. Board of Adjustment*, 56 N.J. Super. 296, 152 A.2d 860, 863, rev'd. on other grounds, 32 N.J. 130, 160 A.2d 30 (1960). However, acting as a de facto notary must be approached with caution because it is a criminal act to falsely assume or pretend to act as a notary. *E.g.*, *Mass. Gen. L. ch. 268 § 33* (1990).

<sup>300</sup> The authority of public officers to undertake notarial acts is sanctioned as acts of notaries ex officio. *Notaries*, 66 C.J.S. § 3 (citing *Wilson v. Simpson*, 68 Tex. 306, 4 S.W. 839 (1887)).

<sup>301</sup> The parties' intention may be expressed in a TPA, an agreement between a party and the electronic notary/trusted entity, or a clearinghouse agreement.

<sup>302</sup> See 12 Am. Jur. *Proof of Facts* § 6, at 288 (1962).

<sup>303</sup> See *Kirk Corp. v. First Am. Title Co.*, 220 Cal. App. 3d 785, 270 Cal. Rptr. 24 (1990); B. Shapiro, *The National Notary Guide and Record Book* 19 (1973).

Notarial record keeping can extend to the notarized documents themselves. It is not unusual for notaries to retain copies of notarized paper documents; retention of notarized documents is a common practice in some European countries, such as France.<sup>304</sup> The statutory requirement in some states that a notary's official acts be available for public inspection may raise privacy issues. Notarial records accessible through electronic means, such as through a public data network, may exacerbate confidentiality and privacy concerns to an extent not previously contemplated by conventional notarial legislation.<sup>305</sup>

**Conformance with evidentiary trends.** Both the rules of evidence and evidentiary procedure have increasingly recognized electronic documents and provided for their authentication.

### Conclusion

The institution of the notary public provides a rich source of structures potentially relevant to increasing the reliability of electronic transactions. New notarial mechanisms should be closely examined and electronic analogs developed and sanctioned. Electronic notarization can provide assurances of reliability comparable to, and for some functions superior to, those provided by conventional notarization. Automation can also breathe new life into the utility of the office of the notary public.

Governments must accommodate electronic business practices by providing appropriate facilities for the notarization of electronic documents. Although aspects of current law may support, or at least tolerate, the automation of the notary public, this subject may be ripe for consideration by the Commissioners on Uniform State Laws and possibly for international rules or conventions projects on judicial assistance, civil procedure, and commercial law—perhaps even a revisiting of the Hague Convention.

---

<sup>304</sup> See Aldisert, *Rambling Through Continental Legal Systems*, 43 U. of Pitt. L. Rev. 935 (Summer 1982).

<sup>305</sup> In light of the privacy concerns raised by public inspection requirements, the automation of notarial records may mandate additional restrictions on access to such records, such as notification, request, sanctions, or supervision. See *American College of Obstetricians v. Thornburgh*, C.A. 82-4336 (E.D. Pa. Mar. 9, 1987) (requirement that petition for abortion be notarized held unconstitutional: "The Plaintiff's concern is that the notary's log, which is by law open to public inspection, [n.16] would contain the name of the minor.").

While payment instructions are not generally considered particularly confidential, remittance advice data is often considered confidential.



## **APPENDIX D - RSA/APPLE A.O.C.E. CERTIFICATE APPLICATION FORM**

The RSA/Apple A.O.C.E. Certificate Application Form is on the next page.

# APPENDIX D - RSA/APPLE A.O.C.E. CERTIFICATE APPLICATION FORM

Untitled Request	
<b>Signer Approval Request Form</b>	
Send notarized form to: RSA Certification Services, 100 Marine Parkway, Redwood City, California 94065 U.S.A.	
Below is the Encoded Signer Information for John Doe ("Applicant"), created on Friday, November 19, 1993. Applicant information: John Doe, 1234 Any Street, Any Town, Any State, 00000, US. After acceptance, send the Signer Approval file to: John Doe, 1234 Any Street, Any Town, Any State, 00000, United States	
<b>Encoded Signer Information:</b> 62+036pgg80ka0g+00/72c8b604gc0q10g3+60ilac/gsc0c0/+1a+0b2c2j0c+g60/324hg203061 84+09gigbef4g56t3+ehij249g+s3061840s9gggbef4g58rrnd//hgc0m0/+1a+092c7j2chj6gg4 2rjp4+9n8sj5clq3249g+s3061840c9ggi jfd+n20h3fck/5/c0d0/4il+i8grrgq08+042g00qb00 /4g0i+03/j/+55+v969e+jik0dhjdjnn0ds7095b/p8mq8ej3iudplt8ufu5efp6vgrg29g06geu+c0 89ji8l88alhma598q++ip6rmcer/pi8908+g200+k+nj0686+4l8ci46uthg2+82646402g00000cs 38e9gn6p9ga830iak6923fe//+0k0j2ha08c0000+v99nmgrh08hmma39h68pj882+dpsi0krke9im at0d85n7i82kdt rms3a+dpsi0krkc5q6a39g60/30c0da1n6it35cgg56t3+ehin6c0d0/4il+i8gr rgq08+0g2g00q+03/d6j m23g+7b5n2j39a2kuhpk iuh+cm5k+/1814pfc+e/6alb9j0uehmafugk+0 9k6msv5ljmj6ibrmk70p2eti0+7+njj4strlc0j8	
<b>USE OF DISSIGN™ IS SUBJECT TO TERMS SET FORTH IN THE POWERTALK USER'S GUIDE AND LICENSE AGREEMENT, INCLUDING LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTY, WHICH ARE HEREBY INCORPORATED INTO THIS FORM. Applicant acknowledges that he/she has read, understands and agrees to such terms.</b> Signed in the presence of the Notary (Applicant's signature): _____ Date: _____	
<b>Instructions to Notary:</b> 1. Modify this form where necessary to assure compliance with the laws of your jurisdiction. Use the back side of this form if necessary. 2. Notary must fully complete the Acknowledgement below. 3. Identification #1 must be a government-issued, widely recognized form of photo ID, such as a Driver's License or Passport. ID's #2 and #3 do not require a photo, but must each be different forms of ID. Examples: valid government-issued ID, employee ID card, utility or tax bill, major insurance card, and no more than one national credit card. 4. Notary shall not undertake an acknowledgement if they are an agent, co-worker, employer, business associate, beneficiary, spouse, or relative of the Applicant. ..... <b>ACKNOWLEDGMENT</b> ..... State or Commonwealth of _____ County of _____ Country _____ On _____ before me, _____ personally appeared _____ (Applicant) proved to me on the basis of the presentation of three forms of identification listed below to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same, and that by his/her signature on the instrument the person executed the instrument in my presence. ID #1 (with photograph) Type: _____ Identifying Number: _____ Expiration Date: _____ ID #2 Type: _____ Identifying Number: _____ Expiration Date: _____ ID #3 (different type than #2) Type: _____ Identifying Number: _____ Expiration Date: _____ Witness my hand and official seal. Notary's Signature _____ Notary's Name (print or type) _____ Notary's Address: _____ (Seal/Stamp) Notary's Phone: _____ My Commission Expires: _____	



## **APPENDIX E - SAMPLE POLICIES**

### **APPENDIX E.1. - M.I.T "MID-RANGE" POLICY STATEMENT**

#### **0. PCA Scope Statement**

- a description of the community this PCA serves

The [mid-range] PCA is intended to provide certification services to the educational and business community. It is intended for those organizations who wish to have their affiliates identified, but wish to employ identification criteria which are less stringent than the [high-end] PCA. Specifically CAs under this PCA are not obligated to use special purpose hardware for signing end-user certificates and may use their discretion as to the mechanism which is employed to identify an individual prior to signing a certificate for them.

It is expected that CAs under this PCA will make good faith efforts both to protect their private component against unauthorized disclosure as well as to identify individuals prior to signing a certificate for them.

#### **1. PCA Security & Privacy**

- technical and procedural security measures employed by the PCA
- measures taken by the PCA to protect the privacy records maintained in conjunction with certification

This PCA will use appropriate hardware, such as the BBN SafeKeyper(TM) or similar Certificate Signature Unit (CSU), for protecting the secret component of its key pair.

Organizations wishing to be certified by this PCA will need to provide the information necessary to issue them a certificate. This information should be provided via Postal Mail and should be on appropriate corporate stationery. In the event of a conflict, more specific information and proof of incorporation or equivalent may be required to resolve the conflict. This PCA reserves the right to revoke CA certificates of CAs whose name (viewed as a fully qualified DN) conflicts with that of bonafide organizations.

#### **2. Certification Policy for CAs and Individual Users:**

- identity verification procedures for certification applied by the PCA and by CAs
- DN conflict resolution procedures
- certification semantics (e.g., affiliation implications, etc.)
- security measures required of CAs by this PCA
- maximum validity interval for CA and user certificates

CAs are expected to use their own discretion in determining the procedures which are necessary and sufficient to identify end-users in their environment. This PCA does however expect CAs to make good faith efforts to properly identify end-users. End-users are expected to be affiliated with the CA which issues them a certificate, as the CA's name will be in essence part of the end-user's distinguished name. However CAs may apply locally defined conventions, such as specified Organizational Unit identifiers to make clear what affiliation is intended (for example OU=Guest to indicate that a particular end-user is not an employee, but does have some affiliation with the CA's organization). It is recognized that different organizations and CAs will apply different criteria in defining "affiliation"; the act of designating an individual as "affiliated" should not be taken as authorizing the individual to act on the organization's behalf in any legal sense.

CA certificates issued by this PCA will have a validity period of no less than 6 months and no more than 2 years. No requirement is established for end-user certificates issued by the individual CAs.

### 3. CRL Management

- frequency of issue by PCA and CAs (min and max interval)
- where PCA makes CRLs (its own and its CAs) available and how (e.g., in conformance with RFC FORMS)
- provisions for CRL archiving by the PCA and CAs

This PCA requires that an organization issue scheduled CRLs no more frequently than weekly. No requirement is established on the maximum interval between CRL issuance. CAs are however cautioned against overly long periods of time between CRL issuance, but each CA must decide what is appropriate given their environment.

CAs may send new, already signed, CRLs to [E-mail address] which will result in them being stored into the PCA CRL archive server. CAs are expected to shortly thereafter issue a CRL fetch command, via the email archive server, to ensure that their CRL was properly received. The PCA will perform regular backup and system maintenance on the CRL archive host(s), however the CAs are responsible for ensuring that their CRLs are reaching the CRL archive system. The PCA reserves the right to revoke the CA certificate for any CA which fails on an ongoing basis to make a current CRL (even if empty) available.

### 4. Naming Conventions

- PCA-imposed constraints on DNs
- semantics of PCA-imposed constraints, e.g., GUEST, MAILING LISTS ... (*see also* #1 above)

All DNs issued to end-users must be subordinate to the CAs DN. However it is expected that the enforcement of this provision will be done in end-user PEM applications.

### 5. Business Issues

- text of any legal agreements that must be executed between CA/user and the PCA
- fee structure for CAs/users

THIS PCA PROVIDES CERTIFICATION SERVICES ON AN "AS-IS" BASIS WITHOUT WARRANTY. USE OF THIS CERTIFICATE SERVICE IS AT THE SOLE RISK OF THE INDIVIDUAL CAs. The only legal agreement necessary between this PCA and any subordinate CAs will in general be limited to affirmation of this PCAs lack of warranty.

At any point in time a CA is expected to have only one certificate valid with this PCA (with the exception of short periods of time needed to effect a smooth transition from one CA certificate to another). If a CAs private component is lost, compromised or otherwise unavailable, the CAs certificate will be revoked and a new one (with a new public key) will be signed by the PCA. There is NO CHARGE for the first CA certificate issued for a particular DN under this PCA, however there will be a charge of \$XXX for the service of revoking and reissuing a CAs certificate. This charge is designed to act as an incentive for CAs to take proper care in protecting their private component.

Some (or all) Public Key cryptosystems in the United States are patented. By providing certificate service, this PCA is NOT granting any organization the right to use public key technology. It is the responsibility of each CA to ensure that they are using products which are properly licensed or to otherwise obtain the right to use public key technology.



## APPENDIX E.2. - RSADSI "Low Assurance" CA Policy Statement

1993 RSA Data Security, Inc.  
Update: October \_\_, 1993  
Steve Dussé & George Parsons

### 1. PCA Identity

Business Identity: RSA Data Security, Inc.  
100 Marine Parkway  
Redwood City, CA. 94065  
Phone (415) 595-8782  
Fax (415) 595-1873  
ca-info@rsa.com

The above EMail address is for general information regarding the PCA. Please refer to Section 8 on Service Provision regarding the appropriate EMail addresses for the different services that this PCA provides.

This PCA uses the following distinguished name:

countryName= US  
organizationName= RSA Data Security, Inc.  
organizationalUnitName= Low Assurance Certification Authority

The above information is accurate on the date specified at the beginning of this policy statement. RSA reserves the right to make appropriate changes to these policies.

### 2. PCA Scope

The community that this Policy Certification Authority (PCA) will serve is unrestricted. The goal of this PCA is to facilitate the rapid and widespread dissemination of public-key certificates with a relatively low level of identification assurance. The purpose of such dissemination is to allow the immediate use, testing, and evaluation of the technology which utilizes these certificates without the more extensive planning and procedures necessary to implement the higher levels of trust required by most environments. This PCA also operates a Certification Authority (CA) that addresses the needs of the members of the Internet community that have expressed the desire for "anonymous" or "persona" certificates since a name that is requested in a certificate-signing request under this authority need not represent the identity of the requester.

### 3. PCA Security and Privacy

This PCA will utilize best efforts to store and control use of the private component of this PCA's RSA key pair to prevent its compromise. Certificate-signing requests and copies of fulfilled certificates will be stored on a generally unsecured server with the goal of providing this information freely to the Internet community to facilitate testing and to allow preemptive prevention of duplication of names in certificate-signing requests.

### 4. Certification Policy for CAs and Individual Users

This PCA will certify any CA or individual wishing to participate in this hierarchy within the rules set forth by the IPRA and by this PCA statement.

## 4.1 CA Certificates

Any CA wishing to be certified by this PCA must submit a certificate-signing request. Since there is no standard format for CA certificate-signing requests, the CA may opt to utilize the user certificate-signing request format specified in Internet RFC1424 or any format which is mutually agreed to by the requester and this PCA. The request should contain, at a minimum, the distinguished name and public component of the RSA key pair of the CA. Some form of identity verification will be performed to attempt to validate that the requester has the right to use the requested distinguished name. In general, however, such verification will be performed with a low level of assurance. As such it should be noted that it will not be difficult for a dedicated attacker to obtain a certificate with a "fake" name.

The distinguished name and public component contained in a CA certificate-signing request will be checked against a list of the distinguished names and public components contained in certificates already issued by this and other PCAs via a database mechanism provided by the IPRA. A CA certificate-signing request will not be fulfilled if the request contains the same distinguished name and public component as a non-revoked certificate that has already been issued and the validity ranges of the issued certificate and the requested certificate overlap.

CAs in this hierarchy should employ reasonable measures to protect the private components of their RSA key pairs. However, the protection of such private components will generally be a local matter, similar to the protection of the private components of RSA key pairs for users. CAs can issue certificates to subordinate CAs and to end-users within the guidelines set forth in Internet RFC1422, i.e., subject names should be subordinate to the issuer name, CA names must be registered with the IPRA. Certificates created by end-users will not be recognized by this PCA.

## 4.2 Persona User Certificates

A distinct CA in this certification hierarchy will be established by this PCA for the issuance of "persona" certificates to individuals. Any individual wishing to be certified by the "persona" CA must submit a certificate-signing request in the format specified by RFC1424. There will be no identity verification applied by this PCA to the "persona" certificate-signing requests. Distinguished names contained in certificate-signing requests will be checked against a list of the distinguished names contained in certificates already issued by this CA. A certificate-signing request will not be fulfilled if the request contains the same distinguished name as a non-revoked certificate that has already been issued and the validity ranges of the issued certificate and the requested certificate overlap.

Under the "persona" CA, individual distinguished names will be certified on a first-come first-served basis. Since the distinguished names will be subordinate to the issuer (see section 4) there will be no need for name conflict resolution outside of this hierarchy. Since there will be no identity verification applied to the certificate-signing requests, there will be no restrictions made on the content of requested distinguished names outside of the restrictions outlined in section 4. THEREFORE, A CERTIFICATE SIGNED BY THIS CA DOES NOT "VOUCH" FOR ANY BINDING BETWEEN THE REQUESTED DISTINGUISHED NAME AND THE IDENTITY OF ANY ENTITY, REAL OR FICTITIOUS. This CA reserves the right to deny a certificate-signing request or to revoke a user certificate that contains a name that is found to be generally abusive, offensive or in conflict with the registered trademark of an organization or any name which is proven to this PCA to belong to an entity other than the requester unless the requester shows proof of permission to use such trademark or name.



### 4.3 Certificate Validity Intervals

CA and individual "persona" certificate-signing requests will not be fulfilled if the requested start time of the certificate is prior to the time of request or the requested start time of the certificate is greater than sixty (60) days after the time of request. This prevents a CA or user from requesting certificates for validity ranges too far into the past or future while allowing the entities enough time to renew existing certificates. A certificate-signing request will not be fulfilled if the requested validity interval is greater than one (1) year or less than one (1) week.

### 5. CRL Management

Certificate-Revocation Lists (CRLs) will be generated by this PCA and the subordinate "persona" CA periodically. CRLs for this PCA and the "persona" CA will be forwarded to the IPRA for service to the Internet Community. All other subordinate CAs in this hierarchy are required to generate and submit to this PCA a CRL upon initial certification and periodically thereafter such that there always exists a valid CRL for each CA. This PCA will maintain a server to serve CRLs from CAs in this hierarchy and forward submitted CRLs to the IPRA for service to the Internet community. This PCA places no additional restrictions upon the frequency and duration of the CRLs generated by subordinate CAs.

Certificate revocation is initiated by the entity that requested the certificate-signing. Entities should request certificate revocation if they suspect that the private component of their RSA key pair has been compromised, if identifying information contained in the certificate has changed, or if they wish to test functionality associated with revocation.

A CA under this PCA can request certificate revocation by sending a PEM message to this PCA, signed by the CA or by the Organizational Notary (ON) that requested certification for the CA. The PEM message body must unambiguously request certificate revocation for the corresponding CA certificate, e.g. "Please revoke this certificate".

An individual "persona" user can request certificate revocation by sending a PEM message to the "persona" CA signed with the private component of the RSA key pair corresponding to the public component in the certificate to be revoked. The PEM message body must unambiguously request certificate revocation, e.g. "Please revoke this certificate."

If a CA or Persona user revocation request mail header includes a return address, this PCA or "persona" CA, respectively, will provide a PEM confirmation of the revocation request signed by an ON of this PCA or "persona" CA. Once revoked, the requester's certificate serial number will appear in the CRL for this PCA or "persona" CA until the revoked certificate naturally expires.

### 6. Naming Conventions

The issuing authority for this PCA will have the following distinguished name:

countryName= US  
organizationName= RSA Data Security, Inc.  
organizationalUnitName= Low Assurance Certification Authority

The subject names that can appear in CA certificates are constrained only by the policies set forth by the ICA.

The issuing authority for the "persona" CA will have the following distinguished name:

countryName= US  
organizationName= RSA Data Security, Inc.  
organizationalUnitName= Persona Certificate

The subject names that can appear in individual "persona" certificates are constrained in the following manners:

- Subject names must be subordinate to the issuer name (must contain all of the issuer's listed attribute-value assertions, encoded identically),
  - Subject names may only contain a single additional terminal commonName attribute.
- Certificate-signing requests that violate these constraints will be rejected.

## 7. Business Issues

The use of Public-Key Cryptography may be covered by U.S. Patents # 4,405,829; 4,200,770; and 4,218,582; and all foreign counterparts.

Certificates provided under this PCA are provided "as is" without any warranty whatsoever. In no event will RSA be liable to any individual or organization for indirect, incidental, special, consequential or exemplary damages arising out of or related to the use of these certificates, including but not limited to lost profits, business interruption or loss of business information.

### 7.1 Fees

There will be a processing fee for the registration of each CA under this PCA. There will be a processing fee for fulfillment of certificate-revocation requests by CAs under this PCA.

There will be no fee for fulfillment of each individual "persona" certificate-signing request or certificate-revocation request under the Persona CA.

## 8. Service Provision

### 8.1 Certificate-signing Requests

CA certificate signing can be requested by sending a certificate-signing request signed by the CA or by an Organizational Notary for the CA to the following address:

ca-low-request@rsa.com

If a request is rejected, this PCA will send back a PEM message signed by an ON for this PCA which indicates the reason for rejection. Otherwise, if the certificate-signing request is fulfilled, this PCA will send back a message via PEM which includes the signed certificate and a current CRL for this PCA.

Individual "persona" certificate signing can be requested by sending a certificate-signing request (see RFC1424) to the following address:

persona-request@rsa.com

If a request is rejected, the "persona" CA will send back a PEM message signed by an ON for the CA which indicates the reason for rejection. Otherwise, if the certificate-signing request is fulfilled, the "persona" CA will send back a PEM message which includes the signed certificate, issuer certificates necessary to "chain" to the root, and current CRLs for the issuers in the chain.



## 8.2 Certificate-revocation Requests

Certificate revocation for CA certificates is requested by sending a PEM message, signed by the CA or by the Organizational Notary for the CA that requested the certificate, to the following address:  
ca-low-revocation-request@rsa.com

The PEM message body must unambiguously request certificate revocation (e.g. "Please revoke this certificate.") and the message must have a valid signature. An acknowledgment will be sent to the user signed by an ON for this PCA.

A certificate-revocation request will not be fulfilled if the required fee is not received within ten (10) days of the electronic request or credit arrangements have not been made.

Certificate revocation for individual "persona" users is requested by sending a PEM message, signed with the private component corresponding to the public component in the certificate to be revoked, to the following address:

persona-revocation-request@rsa.com

The PEM message body must consist of a single line with the text "Please revoke this certificate." and the message must have a valid signature. An acknowledgment will be sent to the user indicating that the revocation was performed.

## 8.3 Payment

The certificate-signing fee and revocation fee for CAs can be submitted via Postal Money Order or company check or any other form of payment that is mutually acceptable by the CA and this PCA. Payment for certificate signing must be accompanied by the desired subject name or digest of the "to be signed" portion of the certificate-signing request. Payment for certificate revocation must be accompanied by the serial number of the certificate to be revoked. Checks and postal money orders are made payable to:

RSA Data Security, Inc. - Certificate Services

Payment and correspondence can be mailed to:

RSA Certificate Services Center  
RSA Data Security, Inc.  
100 Marine Parkway  
Redwood City, CA 94065  
Phone Number: (415) 595-8782  
Fax Number: (415) 595-1873

Alternate arrangements can be made by writing or calling.

## APPENDIX E.3. - T.I.S. COMMERCIAL PCA POLICY STATEMENT

### PCA Policy Statement of Trusted Information Systems, Inc.

July 1, 1993

#### 1. PCA Identity

The business identity and address is

Trusted Information Systems, Inc.  
3060 Washington Road (Route 97)  
Glenwood, MD 21738  
USA  
301-854-6889  
301-854-5363 (fax)

The e-mail address for correspondence addressed to this PCA is

tis-pca@tis.com

Dr. Stephen D. Crocker is the company officer in charge.

This PCA uses the following distinguished name (DN):

/C=US

/S=MD

/O=Trusted Information Systems PCA

Whenever the context is clear, Trusted Information Systems PCA will also be known as TIS-PCA.

This information is effective now and will continue indefinitely. Adjustments to this information will be made as experience is gained.

#### 2. PCA Scope

TIS-PCA provides certification services to the educational, business, and government communities worldwide. It is intended for those organizations who wish to act in the role of Certification Authority (CA) for the purpose of certifying the binding between a specific user and his/her public key using identification criteria which are reasonable and will encourage the use and availability of the public key technology.

#### 3. PCA Security

It is expected that each CA authorized by TIS-PCA will make a good faith effort both to protect its private key against disclosure. A CA under the TIS-PCA domain will use reasonable and appropriate hardware, software, physical, and procedural protection methods to protect its private key. CAs authorized by TIS-PCA may choose to use special purpose hardware for signing end-user certificates, but are not obligated to do so.

TIS-PCA will exercise due care in ascertaining the identity of organizations and individuals to whom it issues certificates.

#### 4. Certification Policy

TIS-PCA reserves the right to judge the legitimacy and uniqueness of the name used in a certificate and the adequacy of the protection used by the CA. If, in the judgment of TIS-PCA, there is sufficient cause to believe the identity of the certificate holder is incorrectly or ambiguously represented by the distinguished name, TIS-PCA may refuse to issue the requested certificate. If the security of the certificate holder's private key is compromised or the binding between the distinguished name and the private key becomes invalid, TIS-PCA may revoke the corresponding certificate. Whenever TIS-PCA issues a residential certificate, the distinguished name in the certificate must



unambiguously designate a specific individual. The distinguished name must include an address. The address may be residential, professional or electronic.

CAs authorized by TIS-PCA must institute policies and procedures for issuing certificates which provide reasonable assurance that the distinguished names in certificates it issues correspond to the identity of the certificate holder, and that all distinguished names are subordinate to the CA's distinguished name.

#### 5. CRL Management

TIS-PCA requires that a CA organization issue scheduled CRLs on an advertised regular basis. No requirement is established on the minimum or maximum interval between CRL issuance. CAs are cautioned against overly short or long periods of time between CRL issuance, but each CA must decide what is appropriate given their environment. CAs should send new, already signed, CRLs to <tis-pca-crl@tis.com>. Such CRLS will [be] stored in the PCA CRL archive server. CAs are expected to issue a CRL fetch command shortly thereafter, via the email archive server, to ensure that their CRL was properly received. TIS-PCA will perform regular backup and system maintenance on the CRL archive host(s), however the CAs are responsible for ensuring that their CRLs are reaching the CRL archive system. TIS-PCA reserves the right to revoke the CA certificate for any CA which fails on an ongoing basis to make a current CRL (even if empty) available.

#### 6. Naming Conventions

All DN's issued to end-users must be subordinate to the CAs DN. However it is expected that the enforcement of this provision will be done in end-user PEM applications.

TIS-PCA reserves the right to inspect the records of each CA authorized by TIS-PCA to check for compliance with the naming rule.

#### 7. Business Issues

CAs operating with certificates issued by TIS-PCA may not have certificates issued by other PCAs unless the CA is in the process of transitioning from one PCA to another and has so notified both TIS-PCA and the other PCA.

If a CA's private key is lost, compromised or otherwise unavailable, the CA's certificate will be revoked and a new one (with a new public key) will be signed by the TIS-PCA.

CAs will be issued a certificate by TIS-PCA only upon completion of a licensing agreement and payment of fees. The licensing agreement embodies the policies set forth in this document. The fee schedule may change from time to time, but changes in fees will not apply to license agreements in force.

#### 8. Other

THIS PCA PROVIDES CERTIFICATION SERVICES ON AN "AS-IS" BASIS WITHOUT WARRANTY. USE OF THIS CERTIFICATE SERVICE IS AT THE SOLE RISK OF THE INDIVIDUAL CAs. The only legal agreement necessary between TIS-PCA and any subordinate CAs will in general be limited to affirmation of this PCA's lack of warranty.

Some (or all) public key cryptosystems in the United States are patented. By providing certificate service, TIS-PCA is NOT granting any organization the right to use public key technology. It is the responsibility of each CA to ensure that they are using products which are properly licensed or to otherwise obtain the right to use public key technology. Within the United States and Canada, a UNIX-based reference implementation of a privacy enhanced MH mail system, TIS/PEM, is available from TIS.

## TIS PCA Price Schedule

July 1, 1993

The following is the price schedule for certificate issuance and registration with the TIS Policy Certification Authority. This price covers registration service, CRL service, royalties for the use of patented technology and possible additional services to be added later. All prices are subject to change without notice, however, no change will affect current registered organizations during the current year. The following price list is based on a course-grained classification according to the size of the organization. This is designed to avoid the burden of counting the precise number of certificates issued by an organization. For purposes of assigning an organization to a class, either a count of the people in the organization or the gross revenue may be used, whichever is more favorable to the organization. Also, in cases where the estimated size is close to the boundary between classes, the more favorable class will be used. Unless an organization undergoes substantial growth, it's expected that its classification will remain stable from year to year. This price schedule applies to both entire organizations and to subdivisions. For example, a university with 8,000 people falls into class D. However, if the Computer Science Department has 350 people and it registers itself, it can register under class C. Similarly, if a particular section or department of a company wishes to register, it will be treated as a smaller entity. This policy is intended to lower the entry cost for registration. If one portion of a school or company is registered and then the entire school or company registers at a later time, a suitable portion of the original payment will be credited to the new registration.

### TIS PCA Price Schedule - page 2

	Class	Schools	Industry
A	Fewer than 10 people or less than \$1 M annual revenue	\$50/yr	200/yr
B	Between 10 and 100 people or between \$1M and \$10M annual revenue	\$250/yr	\$1,000/yr
C	Between 100 and 1,000 people or between \$10M and \$100M annual revenue	\$1,250/yr	\$5,000/yr
D	Between 1,000 and 10,000 people or between \$100M and \$1B annual revenue	\$5,000/yr	\$20,000/yr
E	Over 10,000 people or over \$1B annual revenue	\$12,500/yr	\$50,000/yr

1993 and 1994 discounts:

All service is free for the rest of 1993.

Prices for 1994 are reduced by 50%. For example, in 1994, the cost of class C registration for an industrial organization is \$2,500.

For further information, please contact

Trusted Information Systems, Inc.  
3060 Washington Road (Route 97)  
Glenwood, MD 21738  
USA  
301-854-6889  
301-854-5363 (fax)  
tis-pca-info@tis.com



## **APPENDIX E.4. - COST INT'L CONSORTIUM PCA POLICY STATEMENT**

**COST Consortium Policy Statement  
COST International Consortium  
Computer Security Technologies AB  
Internet Privacy Enhanced Mail (PEM)  
(Version 1.0)**

This part of this Document is the COST Consortium Policy statement and it is structured according to the PEM RFC 1422, Section 3.4.3:

### **1. COST International PCA: Identity**

COST International consortium will serve as the top level PCA for the COST-PEM system. It will establish a number of national organizations, each serving as national CAs, while COST International Consortium will be the international PCA (located in Sweden). The certificates of the national CAs will be signed by the COST International certificate.

The current postal address of the COST International Consortium is:

**COST Computer Security Technologies AB  
Barnhemsvagen 12  
165 76 Hasselby, Sweden**

Other contacts for the COST International Consortium are:

**Person: Sead Muftic  
E-mail address: sead@dsv.su.se  
Telephone: +46-8-16 16 92  
Fax: +46-8-703-9025**

Currently there is only one international (top level) CA at the E-mail address:

**cost-pem@cost.dsv.su.se**

### **2. COST International PCA: Scope of Activities**

COST International will serve as an international PCA. It will establish and serve a number of lower hierarchical levels CAs. Below COST International there will be a number of national CAs. They will be established in each country.

In case of further interest and widespread use of the COST-PEM system, COST will establish CAs at levels lower than national CAs. In that case their certificates will be signed by national CAs.

This version of the COST-PEM supports PCA and CAs which serve only organizational and residential CAs and users. PERSONA users are not supported, they will be implemented in some of the subsequent versions of COST-PEM.

### **3. COST International PCA: Security and Privacy**

COST consortium and its associated members will use advanced security technologies to protect COST-PEM software and its security parameters. All private keys will be kept encrypted and all

procedures using those keys (to sign certificates) will delete all instances of those keys after usage. Soon, COST smart cards will be used for additional protection of secret keys and signature algorithms.

COST-PEM system will be a part of a larger security system implemented at each workstation where PCA or CA software is used (in local networks). That security system will use special passwords and encryption techniques to protect PEM programs and sensitive information belonging to the PEM system. Each PEM resource will be protected against unauthorized modification, duplication or unauthorized usage.

#### 4. COST International PCA: Certification Policy

In this stage, COST International as the PCA will certify only those lower level PCAs and CAs which are using COST-PEM software. Through specially designed procedures for tuning up the PEM software before its distribution, COST will perform verification of PCAs' and CAs' identities, authorizations, and "locations" in the hierarchy. Therefore COST Consortium will run HIGH ASSURANCE PCA and CA procedures for its customers.

Certification policy will be organized in a strict hierarchy of certificates. This hierarchy will be based on Internet DN conventions and E-mail addressing schemes (RFC 822). RFC 822 addresses are converted to the DNs so that the top level name domain (the rightmost element in the E-mail address) is treated as Country (C), the next lower level sub-domain as Organization (O), the rest of the domain name as Organizational Unit (OU), while the Full Name part of the RFC 822 address is treated as Common Name. In such a way no conflict between DNs may appear. The hierarchy of certificates, uniqueness and verification of DNs and binding of PCA, CAs and users will be enforced through the structure and functioning of the COST-PEM software: the modules will be initialized in such a way to ensure all these requirements.

The COST PCA and other CAs will impose the maximum validity time interval for the issued certificates. That interval (in this version of the COST PEM) is two years.

#### 5. COST International PCA: CRL Management

Certificate revocation will be performed if requested by the subject that possesses the certificate. Subjects should request certificate revocation if they suspect that the private component of the RSA key pair has been compromised, if identifying information contained in the certificate has changed or if the validity interval of the certificate has expired.

The COST PCA and each CA will keep the list of revoked certificates (CRL). Each list will contain:

- a. revoked certificates of subordinate CAs, and
- b. revoked certificates of superior CAs and the PCA.

CRLs will be updated with the expired certificates and with existing current certificates, when [a] new request for a certificate is received.



Contrary to the PEM RFCs specifications, the CRLs will not be distributed through the hierarchy. They will be kept by CAs as the local CRL database. The CRLs will be used to reply to user requests for distribution or verification of particular certificates.

The use of the CRLs will be based on various types of PEM letters, those defined by the RFC 1424 document and some additional letters, needed to support all types of CRL management functions.

## 6. COST International PCA: Naming Conventions

COST PCA, CAs and users' names will be full Internet E-mail addresses. Some regulations, restrictions and mutual hierarchical relations are described in the product documentation.

COST Consortium will try through cooperation with national Internet naming authorities to establish standard ("easy-to-remember") names for PCAs and CAs. They will be either in the form

`cost-pem @ cost.<country>`

or at least in the form

`cost-pem @ cost.<domain>`

## 7. COST International PCA: Business Issues

COST International Consortium will distribute run COST-PEM system on a commercial basis.

The initial contract between COST International consortium and other interested parties will include: (1) CA software to implement the corresponding CA hierarchy for certificate management, (2) user PEM software, (3) manuals with installation and usage instructions, and (4) assistance in setting up the PEM system.

Annual fees will also be charged to cover: (1) operational expenses of the COST PCA and CAs, (2) maintenance of software, (3) signing and verification of certificates, (4) maintenance and usage of the CRLs.

Currently, the suggested price is 2.000 US \$ for the central mail server (CA) and 400 US \$ for each user PEM agent at user workstation. Various volume discount schemes are available, as well as other business arrangements. Currently, in 1993 annual operational fees will not be charged.

## 8. COST International PCA: Other Relevant Aspects

COST-PEM has currently completed its alpha testing stage and it is in its beta testing stage. It has been designed, implemented and tested by COST International according to the current PEM RFCs.

Therefore, this statement is issued on the limited basis, for the limited number of interested parties, to participate the beta testing stage. COST-PEM system is currently offered with the deferred payment, which is due after one month of the trial period, after installation. Within the trial period COST International consortium does not give any guarantees for complete functioning of the system. It will, however, do all possible efforts to give full assistance to customers in setting up and using the system and it will do whatever necessary, eventually, to correct the COST-PEM system.

COST International states that the PEM system was tested to the best of our knowledge and that it will do all the reasonable efforts to correct any errors or mistakes.

For the interested parties (potential customers) the next step would be to specify the interest for installing the PEM system. The E-mail letter should be sent

TO: sead@dsv.su.se,  
SUBJECT: PEM Installation.

The letter should specify:

1. The type of the machine where the E-mail is installed
2. The domain name of the mail server
3. The total number of the local PEM user workstations and their types (PC, Mac, UNIX)

In the reply the customer will receive the total price of the system, terms of deferred payment, and further ordering, shipment, and installation procedures.

COST International Consortium  
Stockholm, Sweden  
1 January 1993



## **APPENDIX E.5. - RFC 1422 OUTLINE FOR PCA POLICY STATEMENTS<sup>1319</sup>**

The policy statement submitted by a prospective PCA must address the topics in the following outline. Additional policy information may be contained in the statement, but PCAs are requested not to use these statements as advertising vehicles.

1. PCA Identity- The DN of the PCA must be specified. A postal address, an Internet mail address, and telephone (and optional fax) numbers must be provided for (human) contact with the PCA. The date on which this statement is effective, and its scheduled duration must be specified.

2. PCA Scope- Each PCA must describe the community which the PCA plans to serve. A PCA should indicate if it will certify organizational, residential, and/or PERSONA CAs. There is not a requirement that a single PCA serve only one type of CA, but if a PCA serves multiple types of CAs, the policy statement must specify clearly how a user can distinguish among these classes. If the PCA will operate CAs to directly serve residential or PERSONA users, it must so state.

3. PCA Security & Privacy- Each PCA must specify the technical and procedural security measures it will employ in the generation and protection of its component pair. If any security requirements are imposed on CAs certified by the PCA these must be specified as well. A PCA also must specify what measures it will take to protect the privacy of any information collected in the course of certifying CAs. If the PCA operates one or more CAs directly, to serve residential or PERSONA users, then this statement on privacy measures applies to these CAs as well.

4. Certification Policy- Each PCA must specify the policy and procedures which govern its certification of CAs and how this policy applies transitively to entities (users or subordinate CAs) certified by these CAs. For example, a PCA must state what procedure is employed to verify the claimed identity of a CA, and the CA's right to use a DN. Similarly, if any requirements are imposed on CAs to validate the identity of users, these requirements must be specified. Since all PCAs are required to cooperate in the resolution of potential DN conflicts, each PCA is required to specify the procedure it will employ to resolve such conflicts. If the PCA imposes a maximum validity interval for the CA certificates it issues, and/or for user (or subordinate CA) certificates issued by the CAs it certifies, then these restrictions must be specified.

5. CRL Management- Each PCA must specify the frequency with which it will issue scheduled CRLs. It also must specify any constraints it imposes on the frequency of scheduled issue of CRLs by the CAs it certifies, and by subordinate CAs. Both maximum and minimum constraints should be specified. Since the IPRA policy calls for each CRL issued by a CA to be forwarded to the cognizant PCA, each PCA must specify a mailbox address to which CRLs are to be transmitted. The PCA also must specify a mailbox address for CRL queries. If the PCA offers any additional CRL management services, e.g., archiving of old CRLs, then procedures for invoking these services must be specified. If the PCA requires CAs to provide any additional CRL management services, such services must be specified here.

6. Naming Conventions- If the PCA imposes any conventions on DNs used by the CAs it certifies, or by entities certified by these CAs, these conventions must be specified. If any semantics are associated with such conventions, these semantics must be specified.

7. Business Issues- If a legal agreement must be executed between a PCA and the CAs it certifies, reference to that agreement must be noted, but the agreement itself ought not be a part of the policy

---

<sup>1319</sup> RFC 1422, § 3.4.3 ("Policy Certification Authorities").

statement. Similarly, if any fees are charged by the PCA this should be noted, but the fee structure per se ought not be part of this policy statement.

8. Other- Any other topics the PCA deems relevant to a statement of its policy can be included. However, the PCA should be aware that a policy statement is considered to be an immutable, long lived document and thus considerable care should be exercised in deciding what material is to be included in the statement.



## Appendix F - LLOYDS COMPUTER INSURANCE POLICY

### Insuring Agt. 1

#### COMPUTER SYSTEMS:

By reason of the Insured having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value as the direct result of

(a) fraudulent input of Electronic Data directly into:

- (1) the Insured's Computer System; or
- (2) a Service Bureau's System; or
- (3) any EFT system; or
- (4) a Customer Communication System; or

(b) the fraudulent modification or the fraudulent destruction of Electronic Data stored within or being run within any of the above systems or during electronic transmission through data communication lines including satellite links to the Insured's Computer system or a Service Bureau's Computer System.

which fraudulent acts were committed by a person who intended to cause the Insured to sustain a loss or to obtain financial gain for himself or any other person.

### Insurance Agt. 2

Insured's Service Bureau Operations: . . . customer having . . . by fraudulent input, modification or destruction or thru data lines . . .

### Insurance Agt. 3

Electronic Computer Instructions: . . . by a person who intended to cause the insured to sustain a loss . . .

### Insurance Agt. 4

Electronic Data and Media: A. malicious destruction or attempted threat of the Insured's Electronic Data by any person while the Electronic Data are stored within the Insured's Computer System or a Service Bureau . . .

B. . . media being lost, damaged or destroyed as the direct result of robbery, burglary, larceny, theft, misplacement or mysterious unexplainable disappearance . . .

### Insurance Agt. 5

Computer Virus: A. Virus . . . while such electronic data are stored within the Insured's Computer System or a Service Bureau Computer System.

B. destruction or attempt thereof of the Insured's Electronic Data . . .

### Insurance Agreement 6

Electronic Communications: transmitted or appear to have been transmitted

- (1) through an Electronic Communication System, or
  - (2) by Tested telex, Tested TWX or similar means of Tested communication
- . . . but which either were not sent by said customer, Automated Clearing House . . . or were fraudulently modified during physical transit . . .

Insurance Agreement 7

Electronic Transmission: . . .

Insurance Agreement 8

Electronic Securities: Central Depository having transferred, paid . . . on the faith of an electronic communication purporting to have been directed by the Insured . . .

Insurance Agreement 9

Forged Telefacsimile: . . . but which Tested instructions were sent without the knowledge or consent of said person and bear a forged Signature.

Insurance Agreement 10

Voice Initiated Transfers: directed to the Insured authorising the transfer of funds . . .

Exclusions include: that covered by the Insured's Financial Institution Bond, an identifiable employee and collusion; loss of potential income, incl. interest dividends, indirect or consequential damages loss of any nature . . .

Not deemed to be excess or co-insurance coverage; apply only as excess over any valid and collectable insurance.

\*\*\*



## **XII. GLOSSARY**

<b>AA:</b>	Attribute Authority
<b>AAA:</b>	American Arbitration Association
<b>ABA:</b>	American Bar Association
<b>ACH:</b>	Automated Clearing House
<b>ADR:</b>	Alternative Dispute Resolution
<b>AFTI:</b>	Automated Tariff Filing and Information System
<b>ANSI:</b>	American National Standards Institute
<b>APA:</b>	Administrative Procedure Act
<b>ASC X12:</b>	ANSI Accredited Standards Committee X12
<b>ATM:</b>	Automated Teller Machine
<b>C.F.R.:</b>	Code of Federal Regulations
<b>CA:</b>	Certification Authority
<b>CCC:</b>	Customs Cooperation Council
<b>CEC:</b>	Commission of the European Communities
<b>CHIPS:</b>	Clearing House for Interbank Payments Settlements
<b>COI:</b>	Community(ies) of Interest
<b>COST:</b>	COST International Consortium
<b>CRD:</b>	Certification Request Data
<b>CRL:</b>	Certificate Revocation List
<b>DES:</b>	Data Encryption Standard
<b>DG:</b>	Directorate-General (of the CEC)
<b>DIS:</b>	Draft International Standard
<b>DMM:</b>	Domestic Mail Manual (USPS)
<b>DN:</b>	Distinguished Name
<b>Draft Rules:</b>	UNCITRAL Draft EDI Statutory Provisions
<b>E&amp;O:</b>	Errors and Omissions
<b>EBT:</b>	Electronic Benefit Transfer
<b>ECMA:</b>	European Computer Manufacturers Association
<b>ECPA:</b>	Electronic Communications Privacy Act
<b>EDGAR:</b>	Electronic Data Gathering, Analysis and Retrieval system
<b>EDI:</b>	Electronic Data Interchange
<b>EFT:</b>	Electronic Funds Transfer
<b>F.D.I.C.:</b>	Federal Deposit Insurance Corporation
<b>FARS:</b>	Federal Acquisition Regulations
<b>FAST:</b>	First Attempt to Secure Trade (TEDIS)
<b>FCA:</b>	Federal Certification Authority
<b>FDA:</b>	Food and Drug Administration
<b>Fed. Reg.:</b>	Federal Register

<b>FIPS:</b>	Federal Information Processing Standards
<b>FIRMR:</b>	Federal Information Resource Management Regulations
<b>FMC:</b>	Federal Maritime Commission
<b>FRA:</b>	Federal Records Act
<b>FRB:</b>	Federal Reserve Board
<b>FSIA:</b>	Foreign Sovereign Immunities Act of 1976
<b>FTC:</b>	Federal Trade Commission
<b>FTCA:</b>	Federal Tort Claims Act
<b>GAO:</b>	General Accounting Office
<b>GOSIP:</b>	Government Open Systems Interconnect Protocol
<b>GSSP:</b>	Generally Accepted System Security Principles
<b>GULS:</b>	Generic Upper Layer Security
<b>HHS:</b>	Department of Health and Human Services
<b>ICC:</b>	International Chamber of Commerce
<b>IOIA:</b>	International Organizations Immunities Act of 1945
<b>IPRA:</b>	Internet Policy Registration Authority
<b>(ISC)<sup>2</sup>:</b>	Information Systems Security Certification Consortium
<b>ISO:</b>	International Standards Organization
<b>ISOC:</b>	Internet Society
<b>ITU:</b>	International Telecommunications Union
<b>IULN:</b>	International Union of Latin Notaries
<b>IVAN:</b>	International Value Added Network
<b>LRA:</b>	Local Registration Agent
<b>MAC:</b>	Message Authentication Code
<b>MFJ:</b>	Modified Final Judgment
<b>Model Law:</b>	UNCITRAL Model Law on International Credit Transfers
<b>NACHA:</b>	National Automated Clearing House Association
<b>NADF:</b>	North American Directory Forum
<b>NARA:</b>	National Archives and Records Administration
<b>NII:</b>	National Information Infrastructure
<b>NIST:</b>	National Institute of Standards and Technology
<b>NSA:</b>	National Security Agency
<b>NVLAP:</b>	National Voluntary Laboratory Accreditation Program
<b>NYCHA:</b>	New York Clearing House Association
<b>ODFI:</b>	Originating Depository Financial Institutions
<b>OMB:</b>	Office of Management and Budget
<b>ONA:</b>	Open Network Architecture
<b>ORA:</b>	Organizational Registration Authority



<b>OSI:</b>	Open Systems Interconnection
<b>P&amp;I:</b>	Protection and Indemnity Clubs
<b>P.T.T.:</b>	Postal Telephone & Telegraph
<b>PKAB</b>	Public Key Accreditation Board
<b>PCA:</b>	Policy Certification Authority
<b>PCMCIA:</b>	Personal Computer Memory Card Industry Association
<b>PEB:</b>	Permanent Editorial Board
<b>PEM:</b>	Privacy Enhanced Mail
<b>PIN:</b>	Personal Identification Number
<b>POS:</b>	Point of Sale
<b>PRA:</b>	Postal Reorganization Act
<b>PRC:</b>	Postal Rate Commission
<b>RDFI:</b>	Receiving Depository Financial Institutions
<b>RFC:</b>	ARPA/Internet Request for Comment
<b>ROOT:</b>	Root, <i>see</i> TLCA
<b>RPOA:</b>	Recognized Private Operating Agency
<b>RSA:</b>	RSA Data Security, Inc.
<b>S.W.I.F.T.:</b>	Society for Worldwide Interbank Financial Telecommunications
<b>SBA:</b>	Small Business Administration
<b>SDR:</b>	International Monetary Fund Special Drawing Rights
<b>SEC:</b>	Securities and Exchange Commission
<b>SSN:</b>	Social Security Number
<b>TBDF:</b>	Transborder Data Flow
<b>TIN:</b>	Taxpayer Identification Number
<b>TIS:</b>	Trusted Information Systems, Inc.
<b>TLCA:</b>	Top Level Certification Authority
<b>TPSP:</b>	Third Party Service Provider
<b>U.C.C.:</b>	Uniform Commercial Code
<b>UCC:</b>	Uniform Commercial Code
<b>U.L.A.:</b>	Uniform Law Annotated
<b>U.S.C.:</b>	United States Code
<b>U.S.C.A.:</b>	United States Code Annotated
<b>UN/EDIFACT:</b>	UN/EDI for Administration Commerce & Transport
<b>UNCID:</b>	Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission
<b>UNCTAD:</b>	United Nations Commission on Trade and Development
<b>UPU:</b>	Universal Postal Union
<b>USCIB:</b>	United States Council for International Business
<b>USPS:</b>	United States Postal Service

### XIII. INDEX

access control statutes, .....	148
access device, .....	266
access devices, .....	151
Accreditation, .....	23, 323
accreditation and certification, .....	325
accuracy of credentials, .....	60
act of God, .....	264
Actions for Fraud, Deceit, and Misrepresentation, .....	179
Administration and Management, .....	29
Administrative Procedure Act, .....	174, 185
ADR, .....	378
Aetna, .....	345
agency relationship, .....	100
agent, .....	100
Agreements, Legislation, Regulation, .....	37
Algorithm, .....	60
Algorithms, .....	42
alternative dispute resolution, .....	378
American Bar Association, .....	288, 326, 361
American Stock Exchange, .....	320
Anderson v. United States Postal Service, .....	201
Anti-Competitive Considerations, .....	136
APA, .....	185
APPENDICES, .....	388
Applicability of the U.C.C., .....	109
Applicant Identification Information, .....	46
apportioning liability, .....	81
Approaches to Apportionment of Liability, .....	81
Appropriate Security, .....	365
appropriation law, .....	171
Archival Methods, .....	77
Article 4A, .....	255
ASC X12, .....	377
ASC X3, .....	377
ASC X9, .....	377
assumption of risk, .....	131
ASSUMPTIONS, .....	12
Assurances, .....	5
ATA Carnet, .....	291, 293
ATFI, .....	86
ATM, .....	263
attorney, .....	278
Attribute and Other Certificates, .....	64
attribute certificate, .....	65, 387
Attribute Certificate-related Information, .....	36
Audit Journal, .....	60

Audit Trail, .....	68
Auditing, .....	24
Authorization, .....	51
Authorization to Expend Funds, .....	170
authorized access, .....	151
Automated clearing house, .....	249
automated teller machine, .....	263
Automatic Data Processing Acquisitions and the FIRMR, .....	232
Availability, .....	15, 16, 39
baby FTC Act, .....	98
bad faith, .....	122
bailee, .....	200
bailment, .....	184
Banks and Financial Services, .....	34, 235
bargaining power, .....	376
battle of the forms, .....	352
BEACON, .....	320
Best Available Security, .....	364
bill of lading, .....	315
Bill of Rights, .....	168
Billing and Accounting, .....	59
Billing for Certificates, CRLs, .....	27
billing resolution, .....	268
Board of Governors of the Federal Reserve System, .....	203
Boston Stock Exchange, .....	320
Boyle v. United Technology Corp, .....	223
Burden of Proof for Negligence, .....	280
CA misrepresentation, .....	98
cap on liability, .....	264
Capitalization, .....	45
Caps on VAN Liability, .....	271
Card Technologies, .....	20
cargo receipt, .....	315
Carriage of Goods by Sea Act, .....	312
CCC, 213, 294	
CEDI-FACT, .....	291, 292, 326
Central Intelligence Agency, .....	189
Certificate application processing, .....	57
Certificate authenticity, .....	46
Certificate Creation, .....	23
Certificate Generation, .....	60
Certificate Hold Notice, .....	71
Certificate Information Change, .....	71
Certificate Issuance Hardware, .....	67
Certificate Issuance Propagation, .....	62
Certificate of Origin, .....	291, 294
Certificate Revocation, .....	68
Certificate Revocation Lists, .....	26, 68
Certificate Validity Period, .....	61
Certificates, .....	25, 35
Certification Authority, .....	5



certification chain, .....	333
Certification Liability, .....	91
Certification Policy, .....	406
Certification Request Data, .....	46
certifications and accreditations, .....	323
Certified Information Systems Security	
Professional, .....	328
Chamber of Commerce, .....	326
Chambers of Commerce, .....	291, 292
Changes in Policy, .....	71
CHIPS, .....	254
CHIPS Rules, .....	254
Chubb group, .....	345
CISSP, .....	328
Clayton Act, .....	137
Clearing House Interbank Payments System, .....	254
Clipper/Capstone, .....	42
CMR, .....	312
COGSA, .....	312
COIs, .....	32
Commerce Clause, .....	166
commercial usage, .....	364, 365
commercially reasonable, .....	374
Common Body of Knowledge, .....	328
common carrier, .....	200
common carriers, .....	93, 297
Communications, .....	35
Communications (Voice and Data), .....	25
Communities of Interest, .....	32, 55
community of interest, .....	346
comparative negligence, .....	237
comparative negligence" basis, .....	236
computer abuse and crime, 3.....	85
computer crime, .....	153
Computer Fraud and Abuse Act, .....	148
Computer Fraud and Abuse Act of 1986, ..	147
Computer III, 302	
Computer Malpractice, .....	134
Computer Security Act of 1987, .....	212
Computer-Related Crime Generally, ....	145
CONCLUSIONS AND	
RECOMMENDATIONS, .....	379
Confidentiality of Certificates, .....	68
Conformance testing, .....	329
consequential damages, .....	42, 119, 246
conspicuous, .....	116
conspiracy, .....	137, 154
Constitutional Issues, .....	161
Constitutional Limitations, .....	32
Consumer Credit Protection Act, .....	267
Consumer Transactions, .....	18, 262
consumers, .....	133, 263, 373, 386
Contract Disputes Act of 1978, .....	229
contract of adhesion, .....	87
contractor defense, .....	224
contributory negligence, .....	318
Controls for Certificate Generation, .....	67
Convention on the Contract for International	
Carriage of Goods by Road, .....	312
copies, .....	307
COST, .....	353
COST Consortium Policy Statement, .....	402
COST Int'l Consortium PCA Policy	
Statement, .....	402
cost-reimbursement contracts, .....	229
Costs and Benefits of Security Standards, ..	368
Council Directive Concerning Liability for	
Defective Products, .....	133
Council of the European Communities, ....	133
CRD, .....	46, 50, 180
Credit Card, .....	269
credit cards, .....	262
Credit reporting, .....	140
crime, .....	134, 145
Criminal, .....	44
Criminal Liability, .....	144
CRL, .....	139, 178
CRL Creation, .....	23
CRL Keys, .....	72
CRL Management, .....	406
CRL retention, .....	77
CRL Updating and Promulgation, .....	74
CRL validity period, .....	72
Cross-certification, .....	38
Customs Cooperation Council, .....	294
Customs Coordination Council, .....	213
Customs Modernization Act of 1993, .....	213
cybernotaries, .....	289
Data Integrity Boards, .....	191
debit, .....	263
Defamation, .....	139
defamatory communication, .....	139
defamatory information, .....	139
DEFINITIONS, .....	4
Delegation, .....	32, 387
Delegation Certificates, .....	65
Department of Commerce, .....	138
Department of State, .....	294
detection of error, .....	243
"diffuse" infrastructure, .....	84
Digital Signature, .....	6, 60, 91, 148, 194, 383
Digital Signature Standard, .....	115, 212
digital signatures, 16, 17, 43, 65, 88, 125, 235,	
262, 282, 286, 330, 338	
Direct Damages, .....	118

Direct Liability in Tort or Contract, ..... 106  
 Directory Services, ..... 26, 43, 110  
 disabling devices, ..... 141  
 Disaster Planning, ..... 39  
 disclaim, ..... 100  
 Disclaimer of Implied Warranties, ..... 116  
 disclaiming express warranties, ..... 112  
 disclaiming implied warranties, ..... 116  
 discretionary function, ..... 223  
 "discretionary function" exception, ..... 185  
 Discretionary Function Exemption, ..... 177  
 dishonor of a check, ..... 140  
 Dispute Resolution Mechanisms, ..... 27  
 Dispute Resolution Procedures, ..... 60  
 Distinguished Name, ..... 52, 353, 392  
 documents of title, ..... 317  
 Duty of Care and Measure of Damage, .... 128  
 Duty of Care and Measure of Damages, .. 238  
 Duty to Assist or Enforce, ..... 43  
 E&O, ..... 345  
 E-COM, ..... 198  
 EBT, ..... 266  
 ECMA, ..... 378  
 economic loss, ..... 101  
 EDGAR, ..... 319  
 EDI and Information Technology Division,  
 ..... 361  
 Education and Training, ..... 26  
 EFTA, 262, 263, 267  
 electronic benefit transfer, ..... 266, 387  
 Electronic Communications Privacy Act of  
 1986, ..... 143  
 Electronic Display Books, ..... 320  
 electronic filing, ..... 319  
 Electronic Fund Transfer Act of 1978, ..... 262  
 electronic mail, ..... 35  
 Employees, ..... 30  
 Enhanced services, ..... 301  
 entrustment, ..... 184  
 error or omission, ..... 320  
 Errors and Delays, ..... 243  
 errors and omissions, ..... 344, 345  
 Escrow Agent, ..... 6, 276, 277  
 Escrow Agents, ..... 276  
 escrow agreements, ..... 277  
 escrowing techniques, ..... 213  
 European Directives, ..... 133  
 Evidence, ..... 44, 57, 296, 325, 383  
 Evra Corp. v. Swiss Bank Corp, ..... 120  
 "Execution" Error, ..... 245  
 expectation damages, ..... 119  
 Expectations, ..... 36  
 experimental products,, ..... 132

Express Warranties, ..... 111  
 F.D.I.C., ..... 208, 210  
 Failure to Observe Customer Instructions, 237  
 Fair Credit Reporting Act, ..... 151  
 false light, ..... 142  
 FAR, ..... 225, 232  
 FCA INFRASTRUCTURE - PROPOSALS  
 AND PARADIGMS, ..... 161  
 FCA Policy Development, ..... 37  
 FCA Threats to the Constitutional Rights of  
 Persons, ..... 168  
 FCC, ..... 298, 299, 303  
 Federal Acquisition Regulation, ..... 225  
 Federal Certification Authority, ..... 1, 8  
 Federal Communications Commission, .... 298  
 Federal Contracting/Federal Acquisition  
 Regulation, ..... 225  
 Federal Contractor Liability, ..... 223  
 Federal Deposit Insurance Corporation, .. 208  
 Federal Emergency Management Agency, 211  
 Federal Government as Provider of FCA  
 Services, ..... 161  
 Federal Information Resource Management  
 Regulation, ..... 212  
 Federal interest computers, ..... 150  
 Federal Register, ..... 86  
 Federal Reserve Act, ..... 206  
 Federal Reserve Bank, ..... 258  
 Federal Reserve Bank of New York, ..... 257  
 Federal Reserve Banks, ..... 205  
 Federal Reserve Board, ..... 266  
 Federal Reserve System, ..... 203  
 Federal Sentencing Guidelines, ..... 159  
 Federal Tort Claims Act, 139, 174, 175, 201,  
 280, 380  
 Federal Trade Commission, ..... 98, 138, 142  
 Federal Trade Commission Act, ..... 137  
 Fedwire, ..... 258  
 Fidelity bond, ..... 344  
 fiduciary, ..... 276, 278, 279, 385  
 fiduciary duty, ..... 206  
 Financial Management Services, ..... 213  
 Financial Rules, ..... 369  
 Financial vs. Non-Financial Security  
 Standards, ..... 369  
 FIPS, ..... 233  
 FIRMR, ..... 212, 232  
 First-level Certifications, ..... 91  
 FOIA, ..... 190  
 Foreign Corrupt Practices Act of 1977, .... 159  
 Foreign Sovereign Immunities Act of 1976, 216  
 Forged Checks, ..... 236  
 forged endorsement, ..... 237



Forgery, .....	67	indemnity, .....	341
Fourth Amendment, .....	169	independent contractor, .....	167, 181
Franchising, .....	141	Information Requirements, .....	12
Fraud and swindles, .....	155	Information Security Committee, .....	361
Fraud by wire, radio, or television, .....	153	Information Technology Fund, .....	173
fraudulent misrepresentation, .....	101	inherently dangerous activities, .....	273
fraudulent statements, .....	154	injurious falsehood or disparagement, ....	139
FRB, .....	259	Insurance, .....	27, 45, 231, 314, 337
FRBNY, .....	257	Insurance Agent-Insured, .....	281
Freedom of Speech - 1st Amendment, .....	168	Insurance Company of North America v. United States Postal Service, .....	201
FSIA, .....	218	insurance coverage, .....	325
FTCA, .....	208	Insurance limits, .....	203
FTS-2000, .....	211	Insurance Risks, .....	338
Funds Transfer, .....	258	intellectual property rights, .....	41
funds transfers, .....	235, 240	INTELSAT, .....	222
General Contract Liability Considerations (Including Damages), .....	109	"interconnection" agreement, .....	274
General Services Administration, .....	210	Interference with Contractual Relations, .....	141
General Services Board of Contract Appeals, .....	226	interference with contractual relationships, .....	141
GLOSSARY, .....	410	intermediaries, .....	274
Good faith, .....	106, 142	intermediary, .....	377
goods, .....	109	international, .....	147
Government Insurance Programs, .....	340	International Bureau of Chambers of Commerce, .....	291
government procurement, .....	12	International Chamber of Commerce, ....	291
Green Book, .....	382	International Information Systems Security Certification Consortium, .....	327
Gross Negligence, .....	136	international organizations, .....	218
GSA, .....	211, 232	International Organizations Generally, .....	214
Guidelines, .....	37	International Organizations Immunities Act of 1945, .....	216
Hadley v. Baxendale,, .....	120	International Organizations Immunity Act, .....	221
Hague Convention Abolishing the Requirements of Legalization for Foreign Public Documents, .....	288	International Relationships, .....	34
Hague-Visby Rules, .....	312	International Standards Organization, .....	215
Hamburg Rules, .....	312	International Telecommunications Union, .....	216, 306
Hardware vs. Software Certificate Generation, .....	67	international transport terminals, .....	308
Harter Act, .....	311	International Union of Latin Notaries, ....	288
hazardous or nuclear risks, .....	230	International Value Added Networks, ....	306
Heil v. United States, .....	183	Internet Policy Registration Authority, ..	378
higher-risk information, .....	325	Interoperability testing, .....	329
holographic signatures, .....	252	Interworking, .....	61
I.N.S. v. Chadha, .....	225	Invasion of Privacy, .....	142
IBCC, .....	291	Investigation, .....	51
ICC, .....	291, 336	Investment Securities, .....	319
Identification, .....	307	IOIA, .....	221
Identification Documents, .....	48	IPRA, .....	336, 378
immunity, .....	216, 218	(ISC) <sup>2</sup> , .....	326, 328
Implied Warranties, .....	114	ISO, .....	52, 377
implied warranty of fitness for a particular purpose, .....	115	ISO 9000, .....	327, 331
implied warranty of merchantability, ...	114	Issuing Certificates, .....	38
Indemnification, .....	45		

ITU,.....	306, 377
IULN,.....	326
IVAN,.....	306
judicial pleadings,.....	13
Key Compromise,.....	70
Key Generation,.....	27
Kozolchyk,.....	315
LEGAL CONSIDERATIONS,.....	79
Legal Infrastructure of the FCA,.....	83
letters of credit,.....	346
liability,.....	22, 383
Liability Convention,.....	308
Liability for Defective Information Technology,.....	127
Liability for Defective Information Technology (Strict Liability),.....	129
Liability for Unauthorized Use of Authen. Instrument,.....	95
Liability of Federal Employees,.....	180
liability of notaries public,.....	287
Liability of the Federal Government for Acts of Private Contractors,.....	181
Liability of the Federal Government Generally,.....	174
limit of liability,.....	309
Limitation on Consequential Damages,...	124
Limitations on Remedies,.....	124
Linking Security,.....	388
Liquidated Damages,.....	125
Lloyd's,.....	344, 345
Lloyds Computer Insurance Policy,.....	408
Louchette Corp. v. Merchants Material Insurance Co.,.....	345
M.I.T "Mid-Range" Policy Statement, ....	392
Mailgram,.....	202
Management of Keys,.....	28
Maritime Law Association,.....	314
Massachusetts,.....	353
"matching" legislation of 1988,.....	190
"matching" of data,.....	187
Matters Related to Signature Verification, .....	235
Medicare program,.....	87
merchantability,.....	116
merger clauses,.....	113
MFJ,.....	299
mis-feasance,.....	104
misdescription,.....	244
misrepresentation,.....	180
Misrepresentation by the CA,.....	98
Misrepresentation by the User,.....	94
Model Agreements,.....	358

Model Global Public Key Infrastructure Rules of Practice,.....	361
Model Law on International Credit Transfers, .....	363
Modification of Final Judgment,.....	299
monopolistic,.....	137
NACHA,.....	249
NACHA's Operating Rules,.....	249
NAFTA,.....	213
Name Subordination,.....	54
naming,..52, 71, 72, 193, 353, 355, 393, 396, 400	
Naming Conventions,.....	406
Naming Registration Authorities,.....	55
National Computer Security Laboratory,.....	326
National Institute of Standards and Technology,.....	212
National Voluntary Laboratory Accreditation Program,.....	212, 330
National Weather Service,.....	177
Negligence,.....	105
negligent misrepresentation,.. 95, 96, 104, 107	
Negligently Undertaking to Provide Security,.....	134
negotiability,.....	380
negotiability of transport documents, ....	316
Networks,.....	269
New York Clearing House Association,...	254
New York Stock Exchange,.....	320
NGO,.....	336
NIST,.....	138, 212, 213
Non-Certification,.....	92
non-feasance,.....	104
non-repudiable,.....	16
Non-Repudiation,.....	9
Non-Repudiation vs. Origin Authentication, .....	73
Nondiscrimination and Fairness,.....	58
Nonrepudiation and Notarization Work Group,.....	288
nonstructural safeguards,.....	301
North American Free Trade Agreement,..	213
Notable FCA Candidates,.....	191
notarial acts,.....	282
Notarial Independence,.....	285
Notaries Public,.....	51, 282
Notarization,.....	10
Notary,.....	10
Notary Public,.....	10, 316
notice,.....	129, 315
Notices,.....	35, 37, 319
notices and warnings,.....	384
nuclear energy hazards,.....	341
number,.....	244, 262, 396, 398



Numbering.....	57
numbers.....	259
NVLAP.....	326, 330
NVLAP Program Handbook.....	330
NYCHA.....	254
ODFI.....	250
OECD.....	145
offers and acceptances.....	88
Office of Federal Procurement Policy, ....	225
Office of Federal Procurement Policy Act.....	225
ONA.....	303
ONP.....	303
Open Network Architecture.....	303
Open Network Provision.....	303
Open Systems, .....	19
Operators of Transport Intermediaries in International Trade.....	307
ordinary care.....	237, 238, 239, 246
Organizational Affiliation.....	55
originals.....	307
OTHER APPROACHES TO MITIGATE LIABILITY.....	323
P&I.....	346
parol evidence rule.....	101
party autonomy.....	371, 373
passport.....	294
passwords.....	152
PCA Identity.....	406
PCA Policy Statements.....	347
PCA Scope.....	406
PCA Security & Privacy.....	406
Pecuniary loss.....	139
PEM Outline.....	353
PEM RFC 1422.....	347
persona.....	269
Persona Certificates.....	65
Personal Presence.....	48
physical harm.....	134
Policies Statements and Agreements, .....	36
Policy and Procedures Creation.....	23
Policy Certification Authorities.....	352
policy registration authorities.....	8
policy statements.....	347, 380
Policy Statements Compared.....	356
Politics of Situating the FCA Within the USPS.....	197
postal matter.....	202
Postal Rate Commission.....	196
Postal Reorganization Act.....	192
PRA.....	192
predatory pricing.....	138
Primary Roles of the FCA.....	23
Privacy.....	169

Privacy Act.....	143, 187
Privilege.....	17
Privileges and Immunities.....	216, 219
privity.....	92, 260
Procurement Policy Act.....	225
Professional Negligence.....	134
Professionals.....	327, 333
Proof and Verification of CRD.....	50
Protests, Disputes and Appeals.....	228
public key, 1, 2, 11, 29, 36, 68, 91, 150, 153, 163, 203, 241, 289, 317, 322, 326, 338, 347, 352, 357, 382, 384, 385, 386	
Public Key Accreditation Board.....	337
public policy.....	374
Pull, .....	74
Punitive Damages.....	126, 136, 218
Push, .....	74
Push vs. Pull, .....	62
quality management program.....	331
RDFI.....	250
real property.....	14
Reason Codes for CRL Issuance.....	76
Recipient.....	95
Recipient v. CA -- Contract.....	102
Recipient v. CA -- Contract Liability, .....	97
Recipient v. CA -- Tort.....	104
Recipient v. CA -- Tort Liability.....	95
Recognized Private Operating Agencies, .....	306
record keeping.....	13
Records, .....	40, 187
registered mail, .....	201
Registrar Accreditation Board.....	332
registration, .....	216, 291
registration activities, .....	215
registration authority, .....	20, 214
registration bodies, .....	332
Registries, .....	34
Regulation E, .....	263, 266
Regulation of United States Telecommunications, .....	299
Reliance Damages, .....	123
Remedies, .....	117
"Remote" FCA Notaries, .....	283
reporting requirements, .....	208
Rescission, .....	123
respondeat superior, .....	181
Restitution, .....	123
restrictive theory, .....	218
Retention Media, .....	77
Retention of CRD and Other Information, .....	58
Retention of Current or Expired Certificates, .....	68
Retention Period, .....	77

Revocation Certificates, .....	26	statute of frauds, .....	89
Revocation of Certificate upon Request of		Statutory Provisions, .....	374
Subject's Agent, .....	69	stock exchange clearing rules, .....	319
RFC 1422, .....	347	stop-payment, .....	237
RFC 1422 Outline for PCA Policy Statements,		strict liability, .....	96, 129, 236
.....	406	Subject-Name Uniqueness, .....	52
RICO, .....	156	Subsidiary (Civil) Liability Issues, .....	136
Right or Privilege, .....	55	super notaries, .....	285, 289
Risk Pools, .....	45	Supremacy Clause, .....	90, 207
risks, .....	338	survey, .....	22
Robinson-Patman Antidiscrimination Act,		Survey of Computer Crime Statutes, .....	147
.....	137	Survey of Relevant Non-Computer-Specific	
Role of Security Procedures, .....	241	Statutes, .....	153
Root Authorities, .....	20	Survey of Security Definitions, .....	371
RPOA, .....	306	SURVEY OF, AND APPROACHES TO,	
RRX Industries v. Lab-Con, Inc.,.....	110	TRUSTED ENTITY LIABILITY, .....	235
RSA, .....	353	system rules, .....	375
RSA Commercial Hierarchy, .....	348	T.I.S. Commercial PCA Policy Statement, .....	399
RSA/Apple A.O.C.E. Certificate Application		tax and treasury information, .....	13
Form, .....	391	telegraph, .....	99, 183
RSADSI "Low Assurance" CA Policy		Tempest, .....	329
Statement, .....	394	testing, .....	329
S.W.I.F.T., .....	260	The Certificate Application Process, .....	46
safe deposit, .....	281	The Federal Government as Contractor for	
SCOPE, .....	2	FCA Services, .....	223
searches and seizures, .....	169	The United Nations Convention on the	
Searches and Seizures - 4th Amendment, .....	169	Liability of Operators of Transport	
SEC, .....	319	Terminals in International Trade, .....	308
Second-Level Certification Liabilities, .....	106	Third Party Beneficiaries, .....	375
Second-level Certifications, .....	91	Third Party Service Providers, .....	34
Section of Science and Technology, .....	361	"tie-in" arrangements, .....	138
Securities and Exchange Commission, .....	319	Time and Date Stamping, .....	25, 78
security procedures, .....	241	time and date stamping, .....	282
Security Requirements, .....	363	time stamping, .....	46, 387
Security-Relevant Standards, .....	377	Time Stamps, .....	66
self insurance, .....	345	time/date stamping, .....	10
Self-Insurance Rule, .....	172	Timeliness and Accuracy, .....	57
Self-Signed Certificates, .....	66	Tort Liability Considerations, .....	126
"Sender" Errors, .....	243	TPSP, .....	16
sensitive government documents, .....	12	Trading Partners, .....	10
Separation of Powers, .....	163	transfer of title, .....	318
service, .....	130	trust functionality, .....	315
Sherman Act, .....	136	Trust Models, .....	39
signature, .....	241, 320	Trusted Information Systems, Inc.,.....	353, 399
Social Security Administration, .....	139	Trusted Third Party, .....	10
Society for Worldwide Interbank Financial		Trustee and Trustor, .....	278
Telecommunications, .....	260	Trustworthiness of Verifier, .....	50
sovereign immunity, .....	185, 201, 218, 342	Truth-in-Lending Act, .....	262, 267
specialized agencies, .....	219	Tucker Act, .....	174, 182, 280
Specific Performance, .....	123	U.C.C. Article 4A, .....	240
Sponsor Certificates, .....	65	U.C.C. Article 8, .....	319
standard of care, .....	317	U.C.C. Articles 3 & 4 (Checks),.....	235
Standards, .....	43	U.N. Charter, .....	219



U.N.'s specialized agencies, .....	220
U.S. Customs Service, .....	213
UN/ECE/WP.4, .....	378
unauthorized access, .....	146, 147
UNCITRAL, .....	361
UNCITRAL Model Law on International Credit Transfers, 235	
unconscionable, .....	113
underwriters, .....	339
Underwriters Laboratories, .....	107, 326, 333
Uniform Commercial Code, .....	97
United Nations, .....	215, 219
United Nations Commission on International Trade Law, .....	361
United States Constitution, .....	143
United States Postal Service, .....	191
United States v. Morris, .....	148
unsophisticated user, .....	117
USCIB, .....	294
User Agreement, .....	87
User v. CA -- In Contract, .....	98
User v. CA -- In Tort, .....	101
user-ID/passwords, .....	152
USPS, .....	191
validation, .....	329
Validity Period, .....	61
Value Added Networks, .....	269
VAN, .....	269, 274, 376
VAN Interconnection Agreements, .....	274
VANs, .....	34
Variation by Agreement, .....	371
Vault & Safe Deposit Boxes, .....	281
verification of identity, .....	243
Vicarious Liability, .....	107
Virtual Certificates, .....	65
Visby Protocol, .....	312
Vouch, .....	11, 395
warehouse receipts, .....	318
warehouseman, .....	317
Warranties Under the U.C.C., .....	111
Warsaw Convention, .....	312
wire transfers, .....	240
written agreement, .....	84
wrongful dishonor, .....	239
X9.F1, .....	387
Zeller v. United States, .....	176







